IP Security

IP-Sicherheit: Was ist das?

IP-Sicherheit (IPSec) ist:

- Die langfristige Lösung für sicheres Arbeiten im Netzwerk.
- Hochwirksamer Schutz für private Netzwerke gegen Angriffe aus dem Internet, bei Beibehaltung der Benutzerfreundlichkeit.
- Eine Familie kryptographiebasierter Schutzdienste und Sicherheitsprotokolle.
- Übermittlungssicherheit zwischen Endpunkten. Die einzigen beiden Computer, die bei der Kommunikation über Informationen zum IP-Sicherheitsschutz verfügen, sind der übertragende und der empfangende Computer.
- Die Möglichkeit, Kommunikation zwischen Arbeitsgruppen, LAN-Computern, Domänenclients und -servern, (Remote-)Zweigniederlassungen, Extranets, Clients mit wechselnden Standorten sowie Fernverwaltung von Computern sicher zu gestalten.

Die in Windows 2000 implementierte IP-Sicherheit basiert auf Industriestandards in Verbindung mit Entwicklungen der Arbeitsgruppe für IP-Sicherheit der IETF (Internet Engineering Task Force).

Auf Richtlinien basierende Sicherheit

Schärfere, auf Kryptographie basierende Sicherheitsmethoden, können den Verwaltungsaufwand möglicherweise stark erhöhen. Windows 2000 umgeht dieses Problem durch Implementierung einer richtlinienbasierten Verwaltung für die Internetprotokollsicherheit (IPSec).

Anstelle von Programmen oder Betriebssystemen verwenden Sie Richtlinien zum Konfigurieren der IPSec. Administratoren für die Netzwerksicherheit können Richtlinien für IPSec konfigurieren: von passenden Richtlinien für einen Einzelcomputer bis hin zu solchen für eine Active Directory-Domäne, Site oder Organisationseinheit. Windows 2000 bietet eine zentrale Verwaltungskonsole, IP-Sicherheitsrichtlinienmanagement, zum Festlegen und Verwalten von IPSec-Richtlinien zur Verfügung. Die Richtlinien können so konfiguriert werden, dass sie unterschiedliche Schutzniveaus für die meisten Typen von elektronischem Datenaufkommen in fast allen bestehenden Netzwerken bieten.

Umfassende Sicherheitsmaßnahmen

Netzwerkangriffe können Systemausfälle, Produktionsverluste und die Gefährdung der Sicherheit vertraulicher Daten zur Folge haben, weshalb der Schutz der Daten vor unbefugter Einsichtnahme und Manipulation höchste Priorität hat.

Strategien zum Netzwerkschutz betreffen im Allgemeinen die auf ein Netzwerk von außerhalb ausgeführten Angriffe, die durch Firewalls, Sicherheitsgateways und Benutzerauthentifizierung bei der Einwahl verhindert werden. Diese Maßnahmen

schützen jedoch nicht vor Angriffen, die innerhalb eines Netzwerks ausgeführt werden.

Die Bereitstellung von Sicherheit ausschließlich über Zugriffssteuerungsmaßnahmen (z. B. durch Verwendung von Smartcards und Kerberos) bieten u. U. keinen umfassenden Schutz, da diese Methoden die Verwendung von Benutzernamen und -kennwörtern einschließen. Computer werden häufig für mehrere Benutzer freigegeben und befinden sich, aufgrund der daraus resultierenden häufigen Anmeldevorgänge, in einem ungesicherten Zustand. Wenn ein Benutzername und Kennwort von einem Angreifer entschlüsselt werden, kann der illegale Zugriff auf Netzwerkressourcen nicht ausschließlich durch auf Zugriffssteuerung basierende Sicherheit verhindert werden.

Sicherheitsstrategien auf physischer Ebene schützen die Netzwerkleitungen und Einwahlknoten vor unberechtigtem Zugriff, sie werden jedoch nicht so häufig angewendet. Der Schutz des Netzwerkpfades insgesamt ist damit nicht gewährleistet, denn die Daten werden von der Quelle zu einem bestimmten Ziel übertragen.

Ein effizienter Sicherheitsplan kombiniert mehrere Sicherheitsstrategien und stellt so einen umfassenderen Schutz bereit. Alle diese Strategien können mit IPSec kombiniert werden. Auf diese Weise wird eine weitere Sicherheitsebene bereitgestellt, mit der sichergestellt ist, dass der sendende Computer Sicherheit für jedes IP-Datenpaket vor der Übertragung zu den Netzwerkleitungen bereitstellt und der empfangende Computer den Schutz erst aufhebt, nachdem das Paket empfangen und überprüft wurde.

Netzwerksicherheit

Die Implementierung von IPSec auf einer IP-Übertragungsebene (Network Layer 3) ermöglicht einen hohen Sicherheitsgrad, der mit geringem Aufwand verbunden ist. Bei der Einrichtung von IPSec sind keine Änderungen an vorhandenen Anwendungen oder Betriebssystemen erforderlich. Folgender Einsatz ist in den Szenarios eines Unternehmens denkbar:

Arbeitsgruppen

Lokales Netzwerk (LAN): Client/Server, Peer-to-Peer

Remotezugriff

mobile Clients, Internetzugang, Extranets, Remotebüros.

Andere, oberhalb von Netzwerkschicht 3 konfigurierte Sicherheitsmechanismen, z. B. SSL (Secure Sockets Layer), stellen Sicherheit nur für SSL-erkennende Anwendungen bereit, z. B. Webbrowser. Alle Anwendungen müssen dahingehend geändert werden, dass eine durch SSL geschützte Datenübertragung möglich ist. Innerhalb der Vermittiungsschicht 3 operierende Sicherheitsmechanismen, z. B. die Verschlüsselung auf der Sicherungsschicht, schützen nur die betreffende Verbindung, aber nicht unbedingt alle Verbindungen des Datenpfades. Aus diesem

Grund ist die Verschlüsselung auf der Sicherungsschicht für die Datensicherheit auf Ende-zu-Ende-Basis in Internet- oder gerouteten Intranetszenarios nicht geeignet.
Die Implementation von IPSec auf Vermittlungsschicht 3 stellt Schutz für alle IP-Protokolle und Protokolle höherer Ebene der TCP/IP-Protokollsuite bereit, z. B. TCP, UDP, ICMP und Raw (Protokoll 255) und sogar benutzerdefinierte Protokolle der IP-Ebene. Der Hauptvorteil der Sicherung von Informationen auf dieser Ebene ist, dass alle Anwendungen und Dienste, die IP für die Datenübertragung verwenden, mit IPSec geschützt werden können, ohne dass Änderungen an den Anwendungen und Diensten erforderlich sind. (Zum Schützen von Nicht-IP-Protokollen müssen die Pakete mit IP eingekapselt werden.)

Kryptographiebasierter Schutz

IPSec schützt die Daten, so dass ihre Entschlüsselung für einen Angreifer unmöglich oder zumindest mit erheblichen Schwierigkeiten verbunden ist. Zum Sichern der Informationen wird eine Kombination aus Algorithmus und Schlüssel verwendet. Durch die Verwendung kryptografiebasierter Algorithmen und Schlüssel wird ein hoher Sicherheitsgrad erlangt. Ein Algorithmus führt den mathematischen Vorgang aus, über den die Informationen gesichert werden; der Schlüssel besteht aus einem Geheimcode oder einer Nummer, die zum Lesen, Modifizieren und Überprüfen der gesicherten Daten benötigt wird.

Über die folgenden IPSec-Funktionen werden Netzwerkangriffe verhindert bzw. in hohem Maß reduziert:

?? Automatische Schlüsselverwaltung
?? Schlüsselerstellung

Um eine sichere Datenübertragung zu gewährleisten, müssen beide Computer denselben, freigegebenen Schlüssel erstellen können, ohne dass dieser über das Netzwerk gesendet werden muss. IPSec verwendet für den Schlüsselaustausch den Diffie-Hellman-Algorithmus, mit dem auch das Schlüsselmaterial für alle anderen Verschlüsselungsschlüssel bereitgestellt wird.

Auf beiden Computern wird die Diffie-Hellman-Berechnung gestartet. Anschließend tauschen die Computer öffentlich und sicher ein Zwischenergebnis aus (mit Hilfe der Authentifizierung). Der tatsächliche Schlüssel wird von keinem der beiden Computer übertragen. Unter Verwendung der für den Austausch freigegebenen Informationen erstellt jeder Computer einen identischen Geheimschlüssel. Erfahrene Benutzer können die Standardeinstellungen für den Schlüsselaustausch und den Datenverschlüsselungsschlüssel ändern.

Schlüssellängen

Bei jeder Erweiterung des Schlüssels um ein Bit verdoppelt sich die Anzahl der möglichen Schlüssel, wodurch es zunehmend schwieriger wird, den Schlüssel aufzulösen. Bei der Aushandlung der Sicherheit mit IPSec zwischen den beiden Computern werden zwei Arten von freigegebenen Geheimschlüsseln erzeugt: Hauptschlüssel und Sitzungsschlüssel. Die Hauptschlüssel sind relativ lang; sie umfassen 768 Bit oder 1.024 Bit. Die Hauptschlüssel dienen als Quelle, von der die Sitzungsschlüssel abgeleitet werden. Sitzungsschlüssel werden nach einem

Standardverfahren aus dem Hauptschlüssel abgelaufen. Hierbei ist je ein Sitzungsschlüssel für die einzelnen Verschlüsselungs- und Integritätsalgorithmen erforderlich.

Dynamische Erstellung neuer Schlüssel

Neue Schlüssel können von IPSec während einer Datenübertragung automatisch erstellt werden. Dadurch wird verhindert, dass ein Angreifer sämtliche übertragenen Daten mit einem einzelnen entscheidenden Schlüssel entschlüsseln kann. Erfahrene Benutzer können die Standardschlüsselintervalle ändern.

Sicherheitsdienste

Integrität

Integrität schützt die Informationen während der Übertragung vor unbefugten Änderungen und stellt somit sicher, dass die gesendeten Informationen den Empfänger in unverändertem Zustand erreichen. Mathematische Hashfunktionen werden dazu verwendet, jedes einzelne Paket eindeutig zu markieren oder zu "signieren". Der empfangende Computer überprüft vor dem Öffnen des Pakets die Signatur. Wenn sich die Signatur (und infolgedessen das Paket) geändert hat, wird das Paket ignoriert, um einen möglichen Netzwerkangriff zu verhindern.

Authentifizierung

Bei der Authentifizierung werden Ursprung und Integrität einer Nachricht durch Bestätigen der Echtheit jedes Computers überprüft. Ein unbekannter Computer, der nicht zuverlässig authentifiziert wurde, ist bezüglich der gesendeten Informationen immer verdächtig. In jeder Richtlinie können mehrere Authentifizierungsmethoden enthalten sein. So wird sichergestellt, dass eine gemeinsame Authentifizierungsmethode für Windows 2000-Domänenmitglieder, für Computer, auf denen nicht Windows 2000 ausgeführt wird, und für Remotecomputer gefunden wird.

Vertraulichkeit (Datenverschlüsselung)

Mit Vertraulichkeit wird gewährleistet, dass die gesendeten Daten ausschließlich den gewünschten Empfänger erreichen. Bei dieser Option wird das ESP(Encapsulating Security Payload)-Format für die IPSec-Pakete eingesetzt. Vor der Übertragung werden die Paketdaten verschlüsselt, wodurch sichergestellt ist, dass die Daten während des Übertragens nicht gelesen werden können, selbst wenn das Datenpaket von einem Angreifer überwacht oder manipuliert wird. Nur der Computer mit dem freigegebenen Geheimschlüssel kann die Daten entschlüsseln und ändern. Mit den US-amerikanischen DES-Algorithmen (Data Encryption Standard) DES und 3DES wird die Vertraulichkeit sowohl für die Aushandlung der Sicherheit als auch für die Übertragung von Anwendungsdaten gewährleistet. Mit CBC (Cipher Block Chaining) werden Muster identischer Datenblöcke innerhalb eines Pakets verborgen, ohne die Datenmenge nach der Verschlüsselung zu erhöhen. Wiederholt auftretende Muster in der Verschlüsselung können zu einer Minderung der Sicherheit führen: Angreifer können unter Umständen Hinweise auf den Verschlüsselungsschlüssel ziehen. Ein Initialisierungsvektor (eine vorangestellte Zufallszahl) wird als erster zufällig ausgewählter Block verwendet, mit dem ein Datenblock ver- und

entschlüsselt wird. Verschiedene zufällig ausgewählte Blocks werden in Verbindung mit dem Geheimschlüssel zum Verschlüsseln jedes einzelnen Blocks verwendet. Damit ist sichergestellt, dass identische Gruppen von ungesicherten Daten in einmalige Gruppen verschlüsselter Daten umgewandelt werden. Weitere Informationen zu den Einstellungen für die Kryptografie finden Sie unter Besondere Vorüberlegungen zur IP-Sicherheit.

Nichtverleugnung

Stellt sicher, dass der Sender einer Nachricht als einzige Person für den Sendevorgang in Frage kommt.

Anti-Replay

Auch als Wiedergabeschutz bezeichnet; mit dieser Funktion wird die Einmaligkeit jedes IP-Datenpakets sichergestellt. Durch einen Angreifer aufgefangene Nachrichten können nicht wiederverwendet oder für einen Verbindungsaufbau benutzt werden um sich Informationen illegal zu erschleichen.

IP-Sicherheitsprotokolle

Sicherheitsprotokolle stellen Daten- und Identitätsschutz für jedes IP-Paket zur Verfügung. Die IP-Sicherheit (IPSec) von Windows 2000 verwendet AH (Authentication Header) und ESP (Encapsulating Security Payload), um diese Dienste zur Verfügung zu stellen.

Authentication Header (AH)

AH bietet Authentifizierung, Integrität und Anti-Replay für das gesamte Paket (IP-Header und die im Paket enthaltenen Daten); AH signiert das gesamte Paket. Daten werden nicht verschlüsselt, so dass keine Vertraulichkeit gegeben ist. Die Daten sind lesbar, können aber nicht geändert werden. AH verwendet HMAC-Algorithmen, um das Paket zu signieren.
Integrität und Authentifizierung werden durch die Positionierung des AH-Headers zwischen dem IP-Header und dem Header des Transportprotokolls (TCP oder UDP) zur Verfügung gestellt.

Encapsulating Security Payload (ESP)

ESP bietet neben Authentifizierung, Integrität und Anti-Replay zusätzlich auch Vertraulichkeit.

ESP signiert das gesamte Paket für gewöhnlich nur dann, wenn die Tunnelfunktion darauf angewendet wird. Normalerweise werden nur die Daten, nicht der IP-Header geschützt.

Sicherheit wird durch das Positionieren des ESP-Headers zwischen dem IP-Header und dem Header des Transportprotokolls (TCP oder UDP) geboten.

Profis können das für die Kommunikation zu verwendende Protokoll durch Konfigurieren von Sicherheitsmethoden in der IP-Sicherheitsrichtlinie auswählen.

IP-Sicherheitsrichtlinien-Agent

Der IP-Sicherheitsrichtlinien-Agent ist eine Funktion auf jedem Computer mit dem Betriebssystem Windows 2000, der in der Liste der Systemdienste erscheint. Der Richtlinienagent ruft die aktive IP-Sicherheitsrichtlinieninformation ab und leitet sie an die anderen IP-Sicherheitsfunktionen weiter, die diese Informationen zum Ausführen von Sicherheitsdiensten benötigen.

Der Richtlinien-Agent wird bei Systemstart automatisch gestartet. Sind keine aktiven IP-Sicherheitsrichtlinien vorhanden, oder kann der Richtlinienagent sich aus irgendeinem Grund nicht mit Active Directory verbinden, fragt er Active Directory weiter nach einer zugewiesenen Richtlinie ab oder überprüft die Registrierung nach einer lokal zugewiesenen Richtlinie.

Aushandlung der IP-Sicherheit

Bevor sichere Daten ausgetauscht werden können, muss zwischen den beiden Computern eine Art Abkommen eingerichtet worden sein. Dieses Abkommen wird als Sicherheitszuordnung bezeichnet.

Eine Sicherheitszuordnung ist die Kombination einer Richtlinie und Schlüsseln, die die allgemeinen Sicherheitsdienste, -mechanismen und Schlüssel festlegen, die für den Schutz der Kommunikation zwischen Endpunkten verwendet werden. Der Sicherheitsparameterindex (SPI) ist dabei ein eindeutiger Identifikationswert in der Sicherheitszuordnung, der der Unterscheidung zwischen mehreren auf dem empfangenden Computer vorhandenen Sicherheitszuordnungen dient. Beispielsweise können mehrere Zuordnungen vorhanden sein, wenn ein Computer mit mehreren anderen Computern gleichzeitig sicher kommuniziert. Dieser Fall ist wahrscheinlich, wenn es sich dabei um einen Datei- oder RAS-Server handelt, der mit zahlreichen Clients verbunden ist. Jedoch kann ein Computer auch über mehrere Sicherheitszuordnungen zu einem einzigen Computer verfügen. In diesen Fällen verwendet der empfangende Computer den SPI, um festlegen zu können, welche Sicherheitszuordnung für die Verarbeitung der eingehenden Pakete genutzt werden soll.

Zum Erstellen dieses Abkommens zwischen zwei Computern hat das IETF eine Standardmethode zur Auswertung von Sicherheitszuordnungen und Schlüsselaustauschvorgängen eingerichtet, die das ISAKMP- (Internet Security Association and Key Management Protocol) und das Oakley-Schlüsselgenerierungsprotokoll kombiniert. Das ISAKMP zentralisiert die Verwaltung von Sicherheitszuordnungen, wodurch Verbindungszeiten verringert werden. Oakley erstellt und verwaltet die für die Informationssicherheit verwendeten authentifizierten Schlüssel.
Dieser Vorgang sichert nicht nur die computerübergreifende Kommunikation, sondern schützt auch Remotecomputer bei der Anforderung eines sicheren Zugangs zu einem Unternehmensnetzwerk bzw. in anderen Fällen, bei denen die Aushandlung für den eigentlichen Zielcomputer (oder Endpunkt) durch einen Sicherheitsrouter oder andere Proxyserver erfolgt. Im letzten Fall, der als ISAKMP-Clientmodus bezeichnet wird, werden die Identitäten der Endpunkte ausgeblendet, um die Kommunikation zusätzlich zu schützen.

Um erfolgreich eine sichere Kommunikation gewährleisten zu können, führt ISAKMP/Oakley einen zweiphasigen Vorgang durch. Bei den einzelnen Phasen wird Vertraulichkeit und Authentifizierung durch eine ausgehandelte Verschlüsselung und Authentifizierungsalgorithmen sichergestellt, auf die sich beide Computer geeinigt haben. Dadurch, dass die Aufgaben auf zwei Phasen verteilt werden, kann die Ver-/Entschlüsselung notfalls mit sehr hoher Geschwindigkeit durchgeführt werden.
Schlüsselaustausch

In dieser Initialisierungsphase richten die beiden Computer zunächst die erste, so genannte ISAKMP-Zuordnung, ein. (Diese Sicherheitszuordnung wird gesondert bezeichnet, um über Unterscheidungsmöglichkeiten für die verschiedenen Zuordnungen in den beiden Phasen zu verfügen.) Oakley bietet Identitätsschutz während dieses Austauschs, wodurch eine vollkommene Vertraulichkeit gewährleistet wird. Diese Maßnahme hilft beispielsweise bei allgemeinen Netzwerkangriffen, bei denen Identitäten missbräuchlich "vorgetäuscht" werden.
Der Vorgang der Sicherheitsaushandlung in dieser Phase setzt sich folgendermaßen zusammen:

Richtlinienaushandlung

Diese legt fest:

- Den Verschlüsselungsalgorithmus: DES, 3DES, 40-Bit DES oder keinen.
- Den Integritätsalgorithmus: MD5 oder SHA.
- Die Authentifizierungsmethode: Öffentliches Schlüsselzertifikat, vorinstallierter Schlüssel oder Kerberos V5 (dem Standard in Windows 2000).
- Die Diffie-Hellman-Gruppe.

Werden Zertifikate oder vorinstallierte Schlüssel für die Authentifizierung verwendet, wird die Identität des Computers geschützt. Wird jedoch die standardmäßige Windows 2000-Methode verwendet, wird die Identität des Computers erst verschlüsselt, wenn die gesamten Identitätsdaten in Schritt 3 verschlüsselt werden.

Schlüsselinformationsaustausch

Dadurch verfügen die einzelnen Computer über die notwendigen Informationen zum Erstellen des geheimen, gemeinsam genutzten Schlüssels - dem Hauptschlüssel - für die ISAKMP-Zuordnung. Die eigentlichen Schlüssel werden dabei nicht ausgetauscht, sondern nur die öffentlichen Informationen, die von Diffie-Hellman zum Erstellen des geheimen, gemeinsam genutzten Schlüssels benötigt werden. Der Oakley-Dienst auf den einzelnen Computern erstellt den Hauptschlüssel, der zum Schutz der Authentifizierung verwendet wird.

Authentifizierung

Der Computers versucht, den Schlüsselinformationsaustausch zu authentifizieren. Ohne die erfolgreiche Authentifizierung kann keine Kommunikation erfolgen. Der Hauptschlüssel wird zusammen mit dem in Schritt 1 ausgehandelten Algorithmus verwendet. Unabhängig der verwendeten Authentifizierungsmethoden werden die Identitätsdaten vor Änderungen und Interpretationen geschützt.

Der initiierende Computer sendet eine Angebotsliste potenzieller Sicherheitsstufen zu den antwortenden Computern. Das antwortende Gerät kann dieses Angebot nicht ändern. Sollte das Angebot geändert werden, wird die Antwort vom initiierenden Gerät zurückgewiesen. Der antwortende Computer sendet dann eine Nachricht, in der das Angebot entweder akzeptiert oder mitgeteilt wird, dass keine Option ausgewählt wurde. Und der Vorgang beginnt von neuem.

Die ausgetauschten Aushandlungsmeldungen werden automatisch erneut fünfmal gesendet. Nach drei Sekunden wird eine ladbare Sicherheitszuordnung eingerichtet, wenn die aktiven Richtlinien eine ungesicherte Kommunikation mit einem nicht-IPSec-fähigen Computer unterstützen. Wird eine ISAKMP-Antwort vor der Zeitüberschreitung empfangen, wird die ladbare Sicherheitszuordnung gelöscht und die standardmäßige Sicherheitszuordnungsaushandlung initiiert. Die potentielle Anzahl der Sicherheitszuordnungen wird nur durch die Systemressourcen begrenzt.
Die ISAKMP-Sicherheitszuordnung dient der zweiten Phase der Sicherheitsaushandlungen.

Datenschutz

Ein Paar Sicherheitszuordnungen werden unter Mitwirkung des IP-Sicherheitsdienstes ausgehandelt und als IPSec-Sicherheitszuordnungen bezeichnet. Das Schlüsselmaterial wird aktualisiert oder neue Schlüssel erstellt, wenn PFS bzw. die Schlüsseleinsätze aktiviert wurde und die ISAKMP-Sicherheitszuordnung abgelaufen ist.
Der Vorgang der Sicherheitsaushandlung in dieser zweiten Phase setzt sich folgendermaßen zusammen:

Richtlinienaushandlung

Diese legt fest:

Das IPSec-Protokoll: AH, ESP.
Den Integritätsalgorithmus: MD5, SHA.
Den Verschlüsselungsalgorithmus: DES, 3DES, 40-Bit DES oder keinen.
Es wird ein allgemeines Abkommen getroffen, und die beiden Sicherheitszuordnungen werden eingerichtet: Eine für die interne und die andere für die externe Kommunikation.

Oakley aktualisiert das Schlüsselmaterial, und es werden neue geheime, gemeinsam genutzte Schlüssel für die Authentifizierung und ggf. Paketverschlüsselung erstellt. Wird ein neuer Schlüssel benötigt, erfolgt ein zweiter Diffie-Hellman-Austausch. Oakley aktualisiert das Schlüsselmaterial des Diffie-Hellman-Austauschs, der während des Schlüsselaustauschs durchgeführt wurde, es sei denn, ein Schlüssel oder eine Sicherheitszuordnung ist abgelaufen.

Die Sicherheitszuordnungen und Schlüssel werden an den IPSec-Treiber zusammen mit dem SPI übergeben.

Die gesamte Aushandlung wird durch die ISAKMP-Sicherheitszuordnung geschützt. Außer dem ISAKMP-Kopfbereich werden in den Paketen alle Nachrichtenpakete

verschlüsselt und dem ISAKMP-Kopfbereich folgt eine Integritätssignatur, die die Nachricht authentifiziert. Oakley verhindert Wiederholungen von Aushandlungsnachrichten und stellt einen Anti-Replay-Schutz bereit.
Der Vorgang zu automatischen Nachrichtenwiederholungen ist nahezu mit dem Vorgang zur Aushandlung bei einem Schlüsselaustausch identisch, wobei es jedoch eine Ausnahme gibt: Tritt bei diesem Vorgang während der zweiten oder nachfolgenden Aushandlungen derselben ISAKMP-Sicherheitszuordnung eine Zeitüberschreitung auf, wird eine neue Aushandlung der ISAKMP-Sicherheitszuordnung durchgeführt. Wird eine Nachricht für die Datenschutzphase empfangen, ohne eine ISAKMP-Sicherheitszuordnung einzurichten, wird diese zurückgewiesen.

Durch die Möglichkeit, eine einzige ISAKMP-Sicherheitszuordnung für mehrere IPSec-Sicherheitszuordnungsaushandlungen zu verwenden, wird der Vorgang zur Sicherheitsaushandlung äußerst schnell durchgeführt. Solange die ISAKMP-Sicherheitszuordnung nicht abgelaufen ist, sind erneute Aushandlungen oder Authentifizierungen nicht notwendig. Die aktive IPSec-Richtlinie legt die Anzahl hierfür fest.

Aushandlung der IP-Sicherheit

Bevor sichere Daten ausgetauscht werden können, muss zwischen den beiden Computern eine Art Abkommen eingerichtet worden sein. Dieses Abkommen wird als Sicherheitszuordnung bezeichnet.

Sicherheitszuordnungen

Eine Sicherheitszuordnung ist die Kombination einer Richtlinie und Schlüsseln, die die allgemeinen Sicherheitsdienste, -mechanismen und Schlüssel festlegen, die für den Schutz der Kommunikation zwischen Endpunkten verwendet werden. Der Sicherheitsparameterindex (SPI) ist dabei ein eindeutiger Identifikationswert in der Sicherheitszuordnung, der der Unterscheidung zwischen mehreren auf dem empfangenden Computer vorhandenen Sicherheitszuordnungen dient. Beispielsweise können mehrere Zuordnungen vorhanden sein, wenn ein Computer mit mehreren anderen Computern gleichzeitig sicher kommuniziert. Dieser Fall ist wahrscheinlich, wenn es sich dabei um einen Datei- oder RAS-Server handelt, der mit zahlreichen Clients verbunden ist. Jedoch kann ein Computer auch über mehrere Sicherheitszuordnungen zu einem einzigen Computer verfügen. In diesen Fällen verwendet der empfangende Computer den SPI, um festlegen zu können, welche Sicherheitszuordnung für die Verarbeitung der eingehenden Pakete genutzt werden soll.

Zum Erstellen dieses Abkommens zwischen zwei Computern hat das IETF eine Standardmethode zur Auswertung von Sicherheitszuordnungen und Schlüsselaustauschvorgängen eingerichtet, die das ISAKMP- (Internet Security Association and Key Management Protocol) und das Oakley-Schlüsselgenerierungsprotokoll kombiniert. Das ISAKMP zentralisiert die Verwaltung von Sicherheitszuordnungen, wodurch Verbindungszeiten verringert werden. Oakley erstellt und verwaltet die für die Informationssicherheit verwendeten authentifizierten Schlüssel.

Dieser Vorgang sichert nicht nur die computerübergreifende Kommunikation, sondern schützt auch Remotecomputer bei der Anforderung eines sicheren Zugangs zu einem Unternehmensnetzwerk bzw. in anderen Fällen, bei denen die Aushandlung für den eigentlichen Zielcomputer (oder Endpunkt) durch einen Sicherheitsrouter oder andere Proxyserver erfolgt. Im letzten Fall, der als ISAKMP-Clientmodus bezeichnet wird, werden die Identitäten der Endpunkte ausgeblendet, um die Kommunikation zusätzlich zu schützen.

Um erfolgreich eine sichere Kommunikation gewährleisten zu können, führt ISAKMP/Oakley einen zweiphasigen Vorgang durch. Bei den einzelnen Phasen wird Vertraulichkeit und Authentifizierung durch eine ausgehandelte Verschlüsselung und Authentifizierungsalgorithmen sichergestellt, auf die sich beide Computer geeinigt haben. Dadurch, dass die Aufgaben auf zwei Phasen verteilt werden, kann die Ver-/Entschlüsselung notfalls mit sehr hoher Geschwindigkeit durchgeführt werden.
Schlüsselaustausch
In dieser Initialisierungsphase richten die beiden Computer zunächst die erste, so genannte ISAKMP-Zuordnung, ein. (Diese Sicherheitszuordnung wird gesondert bezeichnet, um über Unterscheidungsmöglichkeiten für die verschiedenen Zuordnungen in den beiden Phasen zu verfügen.) Oakley bietet Identitätsschutz während dieses Austauschs, wodurch eine vollkommene Vertraulichkeit gewährleistet wird. Diese Maßnahme hilft beispielsweise bei allgemeinen Netzwerkangriffen, bei denen Identitäten missbräuchlich "vorgetäuscht" werden.
Der Vorgang der Sicherheitsaushandlung in dieser Phase setzt sich folgendermaßen zusammen:

Werden Zertifikate oder vorinstallierte Schlüssel für die Authentifizierung verwendet, wird die Identität des Computers geschützt. Wird jedoch die standardmäßige Windows 2000-Methode verwendet, wird die Identität des Computers erst verschlüsselt, wenn die gesamten Identitätsdaten in Schritt 3 verschlüsselt werden.

Schlüsselinformationsaustausch

Dadurch verfügen die einzelnen Computer über die notwendigen Informationen zum Erstellen des geheimen, gemeinsam genutzten Schlüssels - dem Hauptschlüssel - für die ISAKMP-Zuordnung. Die eigentlichen Schlüssel werden dabei nicht ausgetauscht, sondern nur die öffentlichen Informationen, die von Diffie-Hellman zum Erstellen des geheimen, gemeinsam genutzten Schlüssels benötigt werden. Der Oakley-Dienst auf den einzelnen Computern erstellt den Hauptschlüssel, der zum Schutz der Authentifizierung verwendet wird.

Authentifizierung

Der Computers versucht, den Schlüsselinformationsaustausch zu authentifizieren. Ohne die erfolgreiche Authentifizierung kann keine Kommunikation erfolgen. Der Hauptschlüssel wird zusammen mit dem in Schritt 1 ausgehandelten Algorithmus verwendet. Unabhängig der verwendeten Authentifizierungsmethoden werden die Identitätsdaten vor Änderungen und Interpretationen geschützt.

Der initiierende Computer sendet eine Angebotsliste potenzieller Sicherheitsstufen zu den antwortenden Computern. Das antwortende Gerät kann dieses Angebot nicht ändern. Sollte das Angebot geändert werden, wird die Antwort vom initiierenden

Gerät zurückgewiesen. Der antwortende Computer sendet dann eine Nachricht, in der das Angebot entweder akzeptiert oder mitgeteilt wird, dass keine Option ausgewählt wurde. Und der Vorgang beginnt von neuem.

Die ausgetauschten Aushandlungsmeldungen werden automatisch erneut fünfmal gesendet. Nach drei Sekunden wird eine ladbare Sicherheitszuordnung eingerichtet, wenn die aktiven Richtlinien eine ungesicherte Kommunikation mit einem nicht-IPSec-fähigen Computer unterstützen. Wird eine ISAKMP-Antwort vor der Zeitüberschreitung empfangen, wird die ladbare Sicherheitszuordnung gelöscht und die standardmäßige Sicherheitszuordnungsaushandlung initiiert. Die potentielle Anzahl der Sicherheitszuordnungen wird nur durch die Systemressourcen begrenzt.
Die ISAKMP-Sicherheitszuordnung dient der zweiten Phase der Sicherheitsaushandlungen.

Datenschutz

Ein Paar Sicherheitszuordnungen werden unter Mitwirkung des IP-Sicherheitsdienstes ausgehandelt und als IPSec-Sicherheitszuordnungen bezeichnet. Das Schlüsselmaterial wird aktualisiert oder neue Schlüssel erstellt, wenn PFS bzw. die Schlüsseleinsätze aktiviert wurde und die ISAKMP-Sicherheitszuordnung abgelaufen ist.
Es wird ein allgemeines Abkommen getroffen, und die beiden Sicherheitszuordnungen werden eingerichtet: Eine für die interne und die andere für die externe Kommunikation.

Oakley aktualisiert das Schlüsselmaterial, und es werden neue geheime, gemeinsam genutzte Schlüssel für die Authentifizierung und ggf.Paketverschlüsselung erstellt. Wird ein neuer Schlüssel benötigt, erfolgt ein zweiter Diffie-Hellman-Austausch. Oakley aktualisiert das Schlüsselmaterial des Diffie-Hellman-Austauschs, der während des Schlüsselaustauschs durchgeführt wurde, es sei denn, ein Schlüssel oder eine Sicherheitszuordnung ist abgelaufen.
Die Sicherheitszuordnungen und Schlüssel werden an den IPSec-Treiber zusammen mit dem SPI übergeben.

Die gesamte Aushandlung wird durch die ISAKMP-Sicherheitszuordnung geschützt. Außer dem ISAKMP-Kopfbereich werden in den Paketen alle Nachrichtenpakete verschlüsselt und dem ISAKMP-Kopfbereich folgt eine Integritätssignatur, die die Nachricht authentifiziert. Oakley verhindert Wiederholungen von Aushandlungsnachrichten und stellt einen Anti-Replay-Schutz bereit.

Der Vorgang zu automatischen Nachrichtenwiederholungen ist nahezu mit dem Vorgang zur Aushandlung bei einem Schlüsselaustausch identisch, wobei es jedoch eine Ausnahme gibt: Tritt bei diesem Vorgang während der zweiten oder nachfolgenden Aushandlungen derselben ISAKMP-Sicherheitszuordnung eine Zeitüberschreitung auf, wird eine neue Aushandlung der ISAKMP-Sicherheitszuordnung durchgeführt. Wird eine Nachricht für die Datenschutzphase empfangen, ohne eine ISAKMP-Sicherheitszuordnung einzurichten, wird diese zurückgewiesen.

Durch die Möglichkeit, eine einzige ISAKMP-Sicherheitszuordnung für mehrere IPSec-Sicherheitszuordnungsaushandlungen zu verwenden, wird der Vorgang zur

Sicherheitsaushandlung äußerst schnell durchgeführt. Solange die ISAKMP-Sicherheitszuordnung nicht abgelaufen ist, sind erneute Aushandlungen oder Authentifizierungen nicht notwendig. Die aktive IPSec-Richtlinie legt die Anzahl hierfür fest.

Gültigkeitsdauern für Sicherheitszuordnungen

Ist die Schlüsselgültigkeitsdauer für den Haupt- oder Sitzungsschlüssel erreicht, wird die zugehörige Sicherheitszuordnung erneut ausgehandelt. Eine Oakley-Löschmeldung wird an den antwortenden Computer gesendet, um diesen aufzufordern, die ISAKMP-Sicherheitszuordnung als "abgelaufen" zu markieren. Auf diese Weise wird verhindert, dass falsche IPSec-Sicherheitszuordnungen aus älteren Sicherheitszuordnungen erstellt werden. Oakley sorgt für das Ablaufen von ISAKMP-Sicherheitszuordnungen, und der IPSec-Treiber für das Ablaufen von IPSec-Sicherheitszuordnungen.

Ruft der IPSec-Richtlinien-Agent Richtlinienaktualisierungen ab, wird die im IPSec-Treiber gespeicherte IP-Filterliste aktualisiert. Sämtliche mit alten Filtern zugewiesenen und in der Richtlinie nicht mehr vorhandenen Sicherheitszuordnungen werden zusammen mit den alten Filtern im Zwischenspeicher des IPSec-Treibers gelöscht.
Läuft die Sicherheitszuordnung ab, während die Energieverwaltungsfunktion in Windows 2000 aktiviert ist und sich der Computer im Ruhezustand befindet, wird die Sicherheitszuordnung automatisch neu ausgehandelt, sobald das Gerät aktiviert wird. Wird Windows 2000 auf einem der Computer heruntergefahren, entfernt die Oakley-Löschmeldung verbleibende Sicherheitszuordnungen und handelt neue Sicherheitszuordnungen aus, wenn das Gerät die Kommunikation wieder aufnimmt. Wird Windows 2000 nicht ordnungsgemäß heruntergefahren, wird die Oakley-Löschmeldung nicht gesendet. In diesem Fall ist die alte Sicherheitszuordnung möglicherweise noch vorhanden, bis die standardmäßige Ablaufzeit erreicht wird. In diesem Fall müssen die Sicherheitszuordnungen manuell gelöscht werden.

IPSec-Paketverarbeitung

Der IPSec-Treiber nimmt die aktive IP-Filterliste vom IPSec-Richtlinienagent entgegen und überprüft alle ein- und ausgehenden Pakete gegen die Filter in der Liste. Stimmt ein Paket mit dem Filter überein, wird die entsprechende Filteraktion angewandt.

Falls die Filteraktion eine Übertragung zulässt, wird das Paket unverändert empfangen bzw. gesendet. Blockiert die Aktion die Übertragung, wird das Paket verworfen.

Die Verarbeitung der aus- und eingehenden Pakete verwendet die SA und die Schlüssel, die dafür ausgehandelt wurden. Der IPSec-Treiber speichert alle aktuellen SAs in einer internen Datenbank. Wenn mehrere SAs vorhanden sind, verwendet der Treiber den SPI (Security Parameters Index), um die Übereinstimmung der korrekten SA mit dem korrekten Paket zu ermitteln.
Entspricht ein ausgehendes IP-Paket einer Aktion in der IP-Filterliste, bei der die Sicherheit auszuhandeln ist, stellt der IPSec-Treiber das Paket in eine Warteliste und benachrichtigt IKE (Internet Key Exchange), mit dem wiederum die Aushandlung der

Ziel-IP-Adresse für das Paket eingeleitet wird. Falls mehrere ausgehende Pakete für ein bestimmtes Ziel mit einem einzelnen Filter übereinstimmen, bevor die Aushandlung durch IKE abgeschlossen ist, wird lediglich das zuletzt empfangene Paket gespeichert.

Nach Abschluss der Aushandlung liefert IKE die Parameter für die SA an den IPSec-Treiber (auch die Sitzungsschlüssel). Der IPSec-Treiber sichert das ausgehende IP-Paket in der Warteschlange und gibt es zur Übertragung an die Netzwerkkarte weiter. Sollte die Aushandlung fehlschlagen, verwirft der IPSec-Treiber das Paket.
Stimmt ein durch IPSec gesichertes eingehendes Paket mit der IP-Filterliste überein, überprüft der IPSec-Treiber die Integrität des Pakets, nimmt gegebenenfalls die Verschlüsselung vor und wandelt es dann wieder in ein normales IP-Format um. Anschließend überprüft der IPSec-Treiber das Paket erneut gegen den Filter. Auf diese Weise wird sichergestellt, dass nur Datenfluss empfangen wird, der im Rahmen der Aushandlung festgelegt wurde. Wenn das Paket mit dem Filter übereinstimmt, sendet der IPSec-Treiber das Paket an TCP/IP zurück, so dass es an die Anwendung übermittelt werden kann.

Beim Empfang eines nicht gesicherten normalen IP-Pakets überprüft der IPSec-Treiber das Paket gegen alle Filter in der Filterliste. Stimmt das Paket mit einem Filter überein, dessen Filteraktion die IP-Sicherheit erfordert oder das Paket blockiert, wird das Paket verworfen.
Der IPSec-Treiber überprüft alle eingehenden ungesicherten Pakete zunächst gegen die Liste der Filter, mit denen die IPSec-Tunnel festgelegt werden, und dann gegen alle Ende-zu-Ende-Filter (Transportfilter). Der IPSec-Treiber ist nicht in der Lage, bestimmte IP-Pakettypen zu filtern.

Funktionsweise der IP-Sicherheit

In diesem Beispiel wird zur Veranschaulichung die Ausführung von IPSec zwischen zwei Domänencomputern verwendet. Marc arbeitet mit einer Anwendung auf Computer A und sendet eine Nachricht an Matthias.

Der IPSec-Treiber auf Computer A überprüft die IP-Filterliste in der aktiven Richtlinie auf Übereinstimmung mit der Adresse oder der Datenübertragungsart der ausgehenden Pakete.

Der IPSec-Treiber benachrichtigt ISAKMP, um Sicherheitsaushandlungen mit Computer B zu starten.

Der ISAKMP-Dienst auf Computer B erhält eine Anforderung für Sicherheitsaushandlungen.

Beide Computer führen einen Schlüsselaustausch aus und richten ISAKMP SA sowie einen geteilten Geheimschlüssel ein.

Beide Computer handeln die für die Datenübertragung geltende Sicherheitsstufe aus, indem sie ein Paar IPSec-SAs und Schlüssel zum Sichern der IP-Pakete einrichten.
Unter Verwendung des ausgehenden IPSec-SA und -Schlüssels signiert der IPSec-Treiber auf Computer A zum Bereitstellen der Integrität die Pakete und verschlüsselt sie nach dem Aushandeln der Vertraulichkeit.

Der IPSec-Treiber auf Computer A überträgt die Pakete zum Verbindungstyp, der für die Übertragung auf Computer B vorgesehen ist.
Computer B empfängt die gesicherten Pakete und überträgt sie zum IPSec-Treiber.
Unter Verwendung des eingehenden IPSec-SA und -Schlüssels überprüft der IPSec-Treiber auf Computer B die Integritätssignatur und hebt ggf. die Verschlüsselung der Pakete auf.

Der IPSec-Treiber auf Computer B überträgt die entschlüsselten Pakete zum TCP/IP-Treiber, der sie zur empfangenden Anwendung weiterleitet.

Für Tanja und Jan läuft dieser Vorgang unbemerkt ab. Die Verwendung von IPSec ist für die Standardrouter oder Switch im Datenpfad zwischen den beiden Peers nicht erforderlich. Diese leiten die verschlüsselten IP-Pakete automatisch zum Ziel weiter. Bei Verwendung des Routers als Firewall, Sicherheitsgateway oder Proxyserver müssen Spezialfilter aktiviert werden, um die gesicherten IP-Pakete weiterzuleiten.

Virtuelle private Netzwerke mit IPSec

Der gesamte Prozess, vom Einkapseln über das Routen bis zur Entkapselung, wird Tunneln genannt. Tunneling oder Einkapselung "versteckt" das Originalpaket in einem neuen Paket bzw. kapselt es darin ein. Dieses neue Paket weist unter Umständen neue Daten für die Adressierung und das Routing auf, so dass das neue Paket über Netzwerke weitergeleitet werden kann. Wird Tunneling mit Datenschutz kombiniert, sind die ursprünglichen Paketdaten (und auch die ursprünglichen Angaben zu Quelle und Ziel) für abfragende Computer im Netzwerk nicht mehr sichtbar. Das Netzwerk kann ein beliebiges Netzwerk sein, d. h. ein privates Intranet oder das Internet. Erreichen die eingekapselten Pakete ihr Ziel, wird der Einkapselungsheader entfernt und das Originalpaket wird anhand seines Originalheaders an sein endgültiges Ziel gesendet.

Der Tunnel selbst ist der logische Datenpfad, über den die eingekapselten Pakete geleitet werden. Für den ursprünglichen Quell- und Zielpeer ist der Tunnel in der Regel transparent; er erscheint wie jede andere Punkt-zu-Punkt-Verbindung im Netzwerkpfad. Die Peers besitzen keine Informationen zu Routern, Vermittlungen, Proxyservern oder anderen Sicherheitsgateways, die zwischen dem Anfangs- und dem Endpunkt des Tunnels liegen. Wird Tunneling mit Datenschutz kombiniert, können Sie hiermit virtuelle privaten Netzwerke (VPNs) einrichten.

Windows 2000 enthält zwei Arten von Tunneling mit IPSec:

Layer-2-Tunneling-Protokoll (L2TP/IPSec): L2TP zur Verwaltung der Einkapselung und des Tunnels für alle Arten von Netzwerkdatenverkehr, IPSec im Transportmodus zur Gewährleistung der Sicherheit für die L2TP-Tunnelpakete.
IPSec im Tunnelmodus: IPSec selbst für die Einkapselung von IP-Datenfluss.
Zum Einsatz dieser Tunneltypen benötigen Sie gründliche Kenntnisse der jeweiligen Funktionen.
Die eingekapselten Pakete werden im Inneren des Tunnels durch das Netzwerk geleitet. (In diesem Beispiel ist das Netzwerk das Internet.) Bei dem Gateway kann es sich um einen Grenzgateway, der sich zwischen der Außenwelt (dem Internet) und dem privaten Netzwerk befindet, einen Router, eine Firewall oder einen anderen Sicherheitsgateway handeln. Darüber hinaus können Sie den Datenfluss zwischen

weniger vertrauenswürdigen Teilen des Netzwerkes mit Hilfe von zwei Gateways innerhalb des privaten Netzwerkes schützen.

L2TP und IPSec

IPSec und L2TP werden kombiniert, um Tunneling und Sicherheit für IP-, IPX- und andere Pakete durch alle IP-Netzwerke hindurch zu gewährleisten. IPSec kann Tunneling auch ohne L2TP durchführen, dies ist aber nur dann empfehlenswert, wenn einer der Gateways L2TP oder PPTP nicht unterstützt.
Bei L2TP werden die ursprünglichen Pakete zunächst in einen PPP-Rahmen eingekapselt. Anschließend werden die Pakete komprimiert (falls möglich) und in ein UDP-Paket eingekapselt, das dem Port 1701 zugewiesen ist. Das UDP-Paket ist ebenfalls ein IP-Paket. L2TP verwendet daher automatisch IPSec, um den Tunnel zu sichern (basierend auf den Sicherheitseinstellungen in der Benutzerkonfiguration des L2TP-Tunnels). Mit dem IPSec-IKE(Internet Key Exchange)-Protokoll wird die Sicherheit für den L2TP-Tunnel standardmäßig anhand der Authentifizierung auf Grundlage von Zertifikaten ausgehandelt. Bei dieser Authentifizierungsmethode wird die Vertrauensstellung zwischen Quellcomputer und Zielcomputer über Computerzertifikate anstelle von Benutzerzertifkaten überprüft. Sobald die IPSec-Transportsicherheit vorliegt, wird der Tunnel durch L2TP ausgehandelt (einschließlich Komprimierung und Benutzerauthentifizierungsoptionen). Die Zugriffssteuerung wird anhand der Benutzeridentität vorgenommen. L2TP/IPSec ist daher die unkomplizierteste, flexibelste, anpassungsfähigste und sicherste Option für das Tunneling, sowohl für VPNs mit Remotezugriff durch Clients als auch für Gateway-zu-Gateway-VPN-Tunnel.

Zur Konfiguration der L2TP/IPSec-VPN-Remotezugriffsclients verwenden Sie Netzwerk- und DFÜ-Verbindungen. Zur Konfiguration des VPN-Remotezugriffsservers und der Gateway-zu-Gateway-Tunnel verwenden Sie die Konsole von Routing und RAS.

Der Header des Originalpakets wird hier als IP- oder IPX-Header dargestellt. Dieser Header enthält die ursprünglichen und die endgültigen Adressen für die Quelle und das Ziel (Adressen im privaten Netzwerk). Der äußere IP-Header (Neuer IP-Header) umfasst die Quell- und Zieladresse der Tunnelendpunkte (Adressen im öffentlichen Netzwerk). Im L2TP-Header befinden sich Daten zur Tunnelsteuerung. Der PPP-Header gibt das Protokoll des ursprünglichen Pakets an, beispielsweise IP oder IPX.

IPSec-Tunnel

Der wichtigste Grund für den Einsatz des IPSec-Tunnelmodus liegt in der Interoperabilität mit anderen Routern, Gateways oder Endsystemen, die keine Unterstützung für L2TP/IPSec oder die PPTP-VPN-Tunneling-Technologie bieten. Der IPSec-Tunnelmodus wird lediglich bei Gateway-zu-Gateway-Tunneling-Szenarien unterstützt, außerdem bei einigen Server-zu-Server- oder Server-zu-Gateway-Konfigurationen (als erweiterte Funktion). Im Kapitel zu IPSec im Windows 2000 Resource Kit finden Sie ausführlichere Beschreibungen dieser Szenarien und Konfigurationen. Beim VPN-Clientremotezugriff wird der IPSec-Tunnelmodus nicht unterstützt. Verwenden Sie statt dessen L2TP/IPSec oder PPTP.

Die beiden Formate für IPSec-Pakete können auch im Tunnelmodus genutzt werden:

ESP-Tunnelmodus

Der ursprüngliche IP-Header (der Header des Originalpakets) enthält für gewöhnlich die endgültigen Quell- und Zieladressen, während der äußere IP-Header in der Regel die Quell- und Zieladressen von Sicherheitsgateways enthält. Das ESP-Tunnelformat bietet eine starke Integrität und Authentizität für den Datenfluss innerhalb des Tunnels. Der ESP-Tunnel wird hauptsächlich eingesetzt, um den Datenschutz für die Tunnelpakete mit der DES- oder 3DES-Verschlüsselung zu gewährleisten. Der Verschlüsselungsgrad wird in der Filteraktion der Tunnelregel festgelegt. Es ist daher möglich, den Grad Keine Verschlüsselung zu bestimmen, wenn kein Datenschutz für den Datenfluss im Tunnel erforderlich ist.

Die im neuen IP-Header enthaltenen Informationen dienen zum Routen des Pakets vom Ursprung zum Endpunkt des Tunnelziels, normalerweise ein Sicherheitsgateway. Der neue IP-ESP-Header wird nicht durch den Integritätshash geschützt. Mit diesem IETF-RFC kann der Paketheader nach Bedarf durch die Netzwerkkomponenten geändert werden, so dass zusätzliche Dienste zur Verfügung stehen (beispielsweise Ändern der Quell- oder Ziel-IP-Adresse oder Heraufsetzen der Priorität gegenüber anderen Paketen).

AH-Tunnelmodus

Der AH-Tunnelmodus bietet lediglich starke Integrität und Authentizität für den Inhalt des Tunnels, nicht jedoch Datenschutz durch Verschlüsselung.

Das gesamte Paket wird zur Sicherung der Integrität signiert, auch der neue Tunnelheader. Aus diesem Grund können keine Änderungen an der Quell- oder Zieladresse vorgenommen werden, sobald das Paket durch den Quellpunkt des Tunnels gesendet wurde. Bei diesem IETF-RFC sind Änderungen an bestimmten Felder im neuen IP-Header durch Netzwerkkomponenten weiterhin möglich, beispielsweise Ändern der Priorität oder Löschen von fehlgeleiteten oder veralteten Paketen. ESP und AH können für das Tunneln auch kombiniert werden, so dass die Integrität des gesamten Pakets und Vertraulichkeit für das ursprüngliche IP-Paket gewährleistet werden.

Bei IPSec-Tunneln wird die Sicherheit lediglich für den IP-Datenfluss gewährleistet. Dieser Tunnel ist so konfiguriert, dass der Datenfluss zwischen zwei IP-Adressen oder der Datenfluss zwischen zwei IP-Subnetzen geschützt wird. Falls Sie den Tunnel nicht zwischen zwei Gateways nutzen, sondern zwischen zwei Hosts, stimmt die äußere IP-Adresse mit der äußeren IP-Adresse überein. Bei Windows 2000 bietet IPSec keine Unterstützung für protokollspezifische, portspezifische oder anwendungsspezifische Tunnel. Die Konfiguration erfolgt über die Konsole der IPSec-Richtlinie. Hierbei wird eine Sicherheitsregel mit einem Filter (zur Beschreibung des Datenflusses durch den Tunnel), einer Filteraktion (zur Sicherung des Tunnels) und einer Authentifizierungsmethode (für die Endpunkte des Tunnels) festgelegt. Es werden drei Arten der Authentifizierung unterstützt: Zertifikate, freigegebene Schlüssel, Kerberos.

Erstellen eines Planes für die IP-Sicherheit

Ob es sich um eine große Domäne oder eine kleine Arbeitsgruppe handelt, die

Implementierung von IP-Sicherheitsrichtlinien stellt einen Kompromiss zwischen der leichten Bereitstellung von Informationen für eine große Anzahl von Benutzern und dem Schutz sensibler Informationen vor unautorisiertem Zugriff dar.
Zum Erreichen dieses Kompromisses ist Folgendes nötig:
Risikoabschätzung und Bestimmung des angemessenen Sicherheitsniveaus in Ihrer Organisation.

Anzeigen wertvoller Informationen

- Festlegen von Sicherheitsrichtlinien, die Ihren Kriterien der Risikoverwaltung entsprechen und die angezeigten Informationen schützen.
- Festlegen, wie die Richtlinien in der bestehenden Organisation optimal umgesetzt werden können.
- Sicherstellen, dass die erforderlichen Voraussetzungen für Verwaltung und Technologie vorhanden sind.
- Bereitstellung eines sicheren und effizienten Zugriffs auf die entsprechenden Ressourcen für alle Benutzer, je nach deren Bedürfnissen.

Sicherheitserwägungen werden auch dadurch beeinflusst, auf welche Art und Weise der Computer benutzt wird. So kann beispielsweise die erforderliche Sicherheit variieren, je nachdem, ob es sich bei dem Computer um einen Domänencontroller, Webserver, RAS-Server, Dateiserver, Datenbankserver, Intranet- oder Remote-Client handelt. Der Sicherheitsrahmen von Windows 2000 ist so konzipiert, dass er höchsten Sicherheitsanforderungen gerecht wird. Allerdings ist die Software allein ohne sorgfältige Planung und Evaluierung, wirksame Sicherheitsleitlinien, deren Umsetzung, Prüfung sowie die Aufstellung und Zuweisung sinnvoller Richtlinien möglicherweise weniger leistungsfähig.

Es gibt keine genaue Definition der Maßnahmen, die als Sicherheitsstandards gelten. Diese können in Abhängigkeit von den Richtlinien und Infrastrukturen verschiedener Organisationen stark variieren. Folgende Sicherheitsniveaus können als allgemeine Grundlagen für die Planung von IP-Sicherheitsrichtlinen gelten:

Minimale Sicherheit

Computer tauschen keine sensiblen Daten miteinander aus. IP-Sicherheitsrichtlinien sind standardmäßig deaktiviert. Es ist nicht notwendig, IP-Sicherheitsrichtlinien zu deaktivieren.

Standardsicherheit

Computer, vor allem Dateiserver, werden zum Speichern wertvoller Daten eingesetzt. In puncto Sicherheit muss ein Kompromiss gefunden werden, damit sie nicht zum Hindernis für legitimierte Benutzer wird, die versuchen, ihre Aufgaben auszuführen. Windows 2000 bietet Ihnen vordefinierte IP-Sicherheitsrichtlinien, die die Daten schützen, aber diese brauchen nicht unbedingt das höchste Sicherheitsniveau: Client (Nur Antwort) und Server (Sicherheit anfordern). Diese oder ähnliche benutzerdefinierte Richtlinien optimieren die Effizienz, ohne bei der Sicherheit Kompromisse zu machen.

Hohe Sicherheit

Bei Computern, auf denen sich hochsensible Daten befinden, besteht das Risiko des Datendiebstahls oder zufälliger bzw. böswilliger Unterbrechung des Systems (besonders bei Remote-DFÜ-Verbindungen), oder Kommunikation mit öffentlichen Netzwerken. Secure Server (Sicherheit erforderlich), eine vordefinierte Richtlinie, erfordert für allen ein- und ausgehenden Datenverkehr IP-Sicherheitsrichtlinienschutz. Secure Server (Sicherheit erforderlich) enthält hochwirksame Algorithmen für Vertraulichkeit und Integrität, Perfect Forward Secrecy, Schlüsseleinsätze und -Grenzen sowie leistungsfähige Diffie-Hellman-Gruppen. Ungesicherte Kommunikation aufgrund von Computern, die nicht den IP-Sicherheitsrichtlinien entspricht oder die Aushandlung nicht bestanden hat, wird blockiert.

Vordefinierte IP-Sicherheitsrichtlinien

Windows 2000 stellt einen Satz vordefinierter IP-Sicherheitsrichtlinien bereit. Standardmäßig sind alle vordefinierten Richtlinien für Windows 2000-Domänenmitglieder konzipiert. Bei ihrer Verwendung wird keine Folgeaktion ausgeführt, sie können aber auch den Erfordernissen entsprechend angepasst oder als Vorlage zum Festlegen benutzerdefinierter Richtlinien verwendet werden.

Vordefinierte Richtlinien

Client (Nur Antwort)

Diese Richtlinie wird bei Computern verwendet, deren Datenkommunikation überwiegend ungesichert sein sollte. Beispielsweise ist die Verwendung von IPSec auf Intranetclients nicht erforderlich, es sei denn, diese wird von einem anderen Computer angefordert. Diese Richtlinie ermöglicht es dem betreffenden Computer, auf Anforderungen gesicherter Datenübertragung entsprechend zu antworten. Sie enthält eine Standardantwortregel, die die Aushandlung mit IPSec-anfordernden Computern ermöglicht. Sicherheit wird entsprechend der Anforderung auf den Datenverkehr der betreffenden Protokolle und Ports begrenzt.

Server (Sicherheit anfordern)

Diese Richtlinie wird bei Computern verwendet, deren Datenkommunikation überwiegend gesichert sein sollte. Dies kann z. B. ein Server sein, mit dem vertrauliche Daten übertragen werden. Bei Anwendung dieser Richtlinie wird ungesicherter Datenverkehr akzeptiert; indem der Computer Sicherheitsanforderungen an den Sender richtet, versucht er jedoch ständig, weitere Datenübertragungen zu sichern. Diese Richtlinie ermöglicht die vollständige ungesicherte Datenübertragung, wenn der andere Computer nicht IPSec-aktiviert ist.

Sicherer Server (Sicherheit erforderlich)

Diese Richtlinie wird bei Computern verwendet, deren gesamte Datenkommunikation gesichert sein sollte. Dies kann z. B. ein Server sein, der zur Übertragung hochsensibler Daten verwendet wird, oder ein Sicherheitsgateway, der das Intranet gegen Übergriffe von außen schützt. Mit dieser Richtlinie wird der ungesicherte

eingehende Datenverkehr zurückgewiesen und der gesamte ausgehende Datenverkehr gesichert. Ungesicherte Datenübertragung wird nicht zugelassen, selbst bei einem nicht IPSec-aktivierten Peer.
Vordefinierte Regeln
Vergleichbar mit den vordefinierten Richtlinien sieht die Standardantwortregel eine Aktivierung ohne Folgeaktion vor, sie kann jedoch im Bedarfsfall angepasst werden. Sie ist Bestandteil jeder neu erstellten Richtlinie, wird aber nicht automatisch aktiviert. Sie ist für alle Computer geeignet, die keine Sicherheit erfordern, aber in der Lage sein müssen, auf Anforderungen anderer Computer nach gesicherter Datenkommunikation entsprechend zu antworten.

Vordefinierte Filteraktionen

Vergleichbar mit den vordefinierten Regeln sind diese Filteraktionen für eine Aktivierung ohne Folgeaktion vorgesehen, sie können aber auch angepasst oder als Vorlage bei der Erstellung benutzerdefinierter Filteraktionen verwendet werden. Sie stehen zur Aktivierung in jeder neuen oder vorhandenen Regel zur Verfügung:
Sicherheit erforderlich. Hohe Sicherheit. Ungesicherte Datenübertragung ist nicht zugelassen.
Sicherheit anfordern (Optional). Mittlere bis niedrige Sicherheit. Ungesicherte Datenübertragung ist zugelassen, um die Kommunikation mit Computern zu ermöglichen, die IPSec nicht aushandeln (können).

Zuweisen einer IP-Sicherheitsrichtlinie

IP-Sicherheitsrichtlinienverwaltung

Die IP-Sicherheitsrichtlinienverwaltung dient zum Erstellen und Konfigurieren von IP-Sicherheitsrichtlinien durch die Microsoft Management Console (MMC). Sie kann Richtlinien (für Active Directory-Clients) zentral verwalten, Richtlinien lokal verwalten (auf dem Computer, auf dem das Snap-In ausgeführt wird), oder Richtlinien für einen Computer oder eine Domäne fernverwalten.
Sie müssen das Snap-In der MMC-Konsole hinzufügen. Ein Assistent führt Sie durch die korrekte Konfiguration des Snap-In. Die benutzerdefinierte Konsole kann anschließend gespeichert werden, so dass der Zugriff darauf jederzeit möglich ist.
In Active Directory gespeicherte Richtlinien

Ein Gruppenrichtlinienobjekt legt Zugriff, Konfiguration und Benutzungseinstellungen für Konten und Ressourcen fest. IP-Sicherheitsrichtlinien können dem Gruppenrichtlinienobjekt eines Computerkontos, einer Site, Domäne oder Organisationseinheit zugewiesen werden. Wird die IP-Sicherheitsrichtline auf das Gruppenrichtlinienobjekt für das Active Directory-Objekt angewendet, dann wird die IP-Sicherheitsrichtlinie an alle Computerkonten weitergegeben, die von diesem Gruppenrichtlinienobjekt betroffen sind. Weitere Informationen erhalten Sie unter Übersicht über Active Directory.

Bei der Zuweisung einer IP-Sicherheitsrichtlinie ist einiges zu beachten.
IP-Sicherheitsrichtlinien, die für die Domänenrichtlinien gelten, setzen die lokalen aktiven IP-Sicherheitsrichtlinien außer Kraft, wenn der Computer ein Mitglied der Domäne ist.

IP-Sicherheitsrichtlinien, die Organisationseinheiten in Active Directory zugewiesen sind, setzen die Richtlinien auf Domänenebene für alle Mitglieder dieser Organisationseinheit außer Kraft, und die IP-Sicherheitsrichtlinien der niedrigsten Organisationseinheit setzen die IP-Sicherheitsrichtlinien für höhere Organisationseinheiten für alle Mitglieder der betreffenden Einheit außer Kraft. Es erfolgt keine Zusammenführung.

Das Zuweisen von Richtlinien auf der höchsten möglichen Ebene bietet bei geringstem Verwaltungsaufwand die größte Wirkungsbreite.

Die IP-Richtlinie bleibt auch dann aktiv, wenn das Gruppenrichtlinienobjekt, dem sie zugewiesen war, gelöscht wurde. Vor dem Löschen des Richtlinienobjekts müssen Sie die Zuordnung der IP-Richtlinie aufheben. Wenn Sie Richtlinienobjekte löschen und die Richtlinie zugeordnet lassen, geht der IP-Sicherheitsrichtlinien-Agent davon aus, dass er die Richtlinie nicht finden kann, und verwendet ein zwischengespeichertes Exemplar.
Bei der Sicherung und Wiederherstellung der Gruppenrichtlinie in Active Directory müssen aus Gründen der Konsistenz auch die IPSec-Richtlinien berücksichtigt werden.
Der IP-Sicherheitsrichtlinien-Agent prüft Active Directory lediglich auf Aktualisierungen der aktiven oder zugewiesenen IPSec-Richtlinie. Haben Sie neue IPSec-Richtlinien in Active Directory angelegt, oder wurde eine IPSec-Richtlinie geändert und einem Clientcomputer zugewiesen, stellt der Winlogon-Dienst diese Änderungen im nächstfolgenden Abfragezyklus hinsichtlich Änderungen an der Gruppenrichtlinie fest. Dieser Dienst benachrichtigt den IPSec-Richtlinien-Agent und wendet anschließend die Änderungen auf den Clientcomputer an.

Richtlinien für den lokalen Computer

Ein Computer mit Windows 2000 besitzt genau ein lokales Gruppenrichtlinienobjekt (häufig als "Richtlinien für den lokalen Computer" bezeichnet). Mit Hilfe dieses lokalen Gruppenrichtlinienobjekts können die Gruppenrichtlinieneinstellungen auf einzelnen Computern gespeichert werden, unabhängig davon, ob diese Computer zu einer Active Directory-Umgebung oder einer Netzwerkumgebung gehören. Die Einstellungen des lokalen Gruppenrichtlinienobjekts können von den Gruppenrichtlinienobjekten überschrieben werden, die einem Standort, einer Domäne oder einer Organisationseinheit zugeordnet sind. Aus diesem Grund besitzt das lokale Gruppenrichtlinienobjekt den geringsten Einfluss in der Active Directory-Umgebung. In einer Umgebung ohne Netzwerk (bzw. in einer Netzwerkumgebung ohne Windows 2000-Domänencontroller) sind die Einstellungen aus dem lokalen Gruppenrichtlinienobjekt bedeutender, weil sie nicht von anderen Gruppenrichtlinienobjekten überschrieben werden.

Besondere Vorüberlegungen zur IP-Sicherheit

Die folgenden Überlegungen sollen dazu beitragen, die Verwaltung der IP-Sicherheitsrichtlinien zu vereinfachen:

Verschlüsselungsanforderungen bei Windows 2000

Die Verfügbarkeit der IPSec-Verschlüsselungsfunktionen in Windows 2000 unterliegt den Exportbestimmungen der USA sowie gegebenenfalls den Bestimmungen für den Einsatzort. Bei IKE (Internet Key Exchange) dient die Verschlüsselung zum Schutz der Sicherheitsaushandlung, bei der IPSec-Komponente von TCP/IP dagegen zum Schutz von Anwendungsdatenpaketen. Zum Schutz der Aushandlung muss IKE mindestens die DES-Verschlüsselung über die CAPI (Cryptographic API) nutzen können. Um den Datenfluss mit den verschiedenen IPSec-Paketformaten zu schützen, müssen Windows 2000-Computer DES in CAPI einsetzen können.
Mit 3DES bieten die IPSec-Richtlinien einen starken Verschlüsselungsalgorithmus, bei dem die Sicherheit durch Einsatz eines längeren Schlüssels als bei DES erhöht wird. Diese Richtlinie gilt für alle Computer, denen die Richtlinie zugewiesen wird. Bei Windows 2000-Computern wird allerdings das High Encryption Pack benötigt, um den 3DES-Algorithmus ausführen zu können. Erhält ein Computer eine 3DES-Einstellung, ohne dass das High Encryption Pack vorliegt, wird die 3DES-Einstellung in der Verschlüsselungsrichtlinie durch die schwächere DES-Einstellung ersetzt.

Authentifizierung

Wenn die Computer in Ihrem Unternehmen zu einer Windows 2000-Domäne gehören, kann die IPSec-Authentifizierung mit dem Windows 2000-Standardauthentifizierungsprotokoll (Kerberos V5) ausgeführt werden. Für die Datenübertragung im Unternehmensintranet sind keine öffentlichen Schlüsselzertifikate erforderlich.
IP-Filterlisten
Versuchen Sie, allgemeine Filter zu verwenden, um mit einem Filter eine möglichst hohe Anzahl von Computern abzudecken. Verwenden Sie z. B. die Option Beliebige IP-Adresse oder eine IP-Subnetzadresse anstelle der IP-Quell- und Zieladresse des betreffenden Computers.

Legen Sie die Filter fest, mit denen Sie den Datenverkehr in den betreffenden Bereichen Ihres Netzwerks gruppieren und sichern möchten.

Filteraktionen

Um die Datenübertragung mit nicht autorisierten Computern zu verhindern, stellen Sie sicher, dass für nicht benötigte Daten oder nicht IPSec-aktivierte Peers keine Sicherheit ausgehandelt wurde, und verwenden Sie Filteraktionen als blockierende (Blockieren) oder Pass-Through-Richtlinien (Zulassen).
Beim Konfigurieren benutzerdefinierter Sicherheitsmethoden sollte die ESP-Vertraulichkeit nur dann auf Keine gesetzt werden, wenn ein Protokoll höherer Ebene die Datenverschlüsselung bereitstellt.
Bei den Szenarios der Remoteübertragung (einschließlich IPSec-Tunnel) sollte eine Liste mit Sicherheitsmethoden eingerichtet werden, mit denen ein hoher Sicherheitsgrad implementiert wird, wie z. B. die ausschließliche Verwendung von 3DES, kurzem Schlüsseleinsatz (weniger als 50 MB) und Perfect Forward Secrecy für die Haupt- und Sitzungsschlüssel. Dies erhöht den Schutz vor bekannten Angriffen gegen Schlüssel.

RAS-Übertragung

Wenn Sie L2TP verwenden, muss die Liste der Authentifizierungsmethoden Zertifikate enthalten und auf jedem Peer (Remoteclient oder RAS-Server) muss mindestens ein öffentliches Schlüsselzertifikat auf Computerebene konfiguriert sein . Windows 2000-Domänencontroller können zum automatischen Einschreiben von Domänenmitgliedern in einer Zertifizierungsstelle konfiguriert werden.

Zum Schutz vor Netzwerkattacken auf einen RAS-Server sollte die vordefinierte Filteraktion Sicherheit anfordern (oder eine ähnliche benutzerdefinierte Filteraktion) aktiviert sein. Die Optionen Unsichere Komm. mit Computern zulassen, die IPSEC nicht unterstützen und Unsichere Kommunikation zulassen, aber immer mit IPSEC antworten sollten nur mit Vorsicht verwendet werden. Das Zulassen von unsicherem Datenverkehr kann Sicherheitsprobleme verursachen.

Beim Konfigurieren der IP-Filterliste für einen RAS-Server (welcher normalerweise mehrere Schnittstellen und Adressen hat) sollte nicht die Option Eigene IP-Adresse für die Filter gesetzt werden. In diesem Fall wird IPSec versuchen, die Verwendung des betreffenden Filters auf allen Schnittstellen des Servers zu erzwingen. Konfigurieren Sie stattdessen den Filter für die IP-Adresse derjenigen Schnittstelle, die den zu sichernden Datenverkehr sendet und empfängt.

Wenn die Computer in Ihrem Unternehmen remote verwaltet werden, muss der aktiven IP-Sicherheitsrichtlinie eine Regel hinzugefügt werden, mit der verhindert wird, dass der vom internen Netzwerk eingehende über RPCs (Remote Procedure Calls) erfolgende TCP-Datenverkehr gesperrt wird. (Dieser Datenübertragungstyp wird von den RAS-Konfigurationstools von Windows 2000 verwendet). Zum Beispiel:
Die IP-Filterliste der Regel sollte eine ausgehende Adresse des unternehmenseigenen Subnetzes enthalten (es handelt sich um den Standort der Verwaltungskonsole) und eine eingehende Adresse der vom Computer verwalteten internen IP-Adresse. Als Protokolltyp sollte TCP gewählt werden.
Die Filteraktion der Regel sollte die Optionen Unsichere Kommunikation annehmen und Unsichere Kommunikation mit Hostcomputern zulassen, die IPSEC nicht unterstützen zulassen.

SNMP

Wenn ein Computer mit dem SNMP-Dienst ausgeführt wird, muss eine Regel hinzugefügt werden, die das Sperren von SNMP-Nachrichten verhindert.
In der IP-Filterliste sollten die Quell- und Zieladressen des SNMP-Verwaltungssystems und der -agents angegeben werden. Als Protokolltyp sollte UDP (ankommend und abgehend an Port 161 und 162) gewählt werden. Dazu sind zwei Filter erforderlich: einer für UDP an Port 161 (ankommend und abgehend) und der andere an Port 162 (ankommend und abgehend).
Die Filteraktion sollte auf Zulassen eingestellt werden, auf diese Weise wird die Sicherheitsaushandlung gesperrt und jeder der IP-Filterliste entsprechende Datenverkehr wird durchgeleitet.

Sicherheitsgateways

Auf Sicherheitsgateways, Firewalls, Proxyservern, Routern und allen Servern des Intranets, mit denen auch auf das Internet zugegriffen werden kann, müssen spezielle Filter eingerichtet sein, um zu gewährleisten, dass mit IPSec gesicherte

Pakete nicht zurückgewiesen werden. Zum mindesten müssen die folgenden Eingabe- und Ausgabefilter für die Internetschnittstelle des betreffenden Computers festgelegt werden:

Eingabefilter

IP-Protokoll-ID von 51 (0x33) für eingehenden IPSec-AH (Authentication Header)-Datenverkehr.
IP-Protokoll-ID von 50 (0x32) für eingehenden IPSec-EPS (Encapsulating Security Protocol)-Datenverkehr. UDP-Anschluss 500 (0x1F4) für eingehende ISAKMP/Oakley-Aushandlungen.
Ausgabefilter
IP-Protokoll-ID von 51 (0x33) für ausgehenden IPSec-AH (Authentication Header)-Datenverkehr.
IP-Protokoll-ID von 50 (0x32) für ausgehenden IPSec-EPS (Encapsulating Security Protocol)-Datenverkehr. UDP-Anschluss 500 (0x1F4) für ausgehende ISAKMP/Oakley-Aushandlungen.
DHCP-, DNS- und WINS-Dienste; Domänencontroller
Bevor IPSec für Server mit dem oben genannten Funktionsumfang eingerichtet wird, sollten alle IPSec-fähigen Clients festgelegt werden. Die Sicherheitsaushandlung könnte sonst versehentlich fehlschlagen und der Zugang zu den Netzwerkressourcen blockiert werden.

DNS

Bei Angabe von DNS-Namen in einer IP-Filterliste sind im Falle von nicht IPSec-aktivierten DNS-Servern spezielle Richtlinieneinstellungen erforderlich. Andernfalls können IPSec und andere, auf dem Server eingerichtete Dienste den DNS-Computernamen nicht in eine gültige IP-Adresse auflösen.

Richten Sie die IP-Filterliste so ein, dass der Datenverkehr zwischen Computer und DNS-Server von den IPSec-Sicherheitserfordernissen unabhängig ist:
Legen Sie als Quelladresse Eigene IP-Adresse fest.
Legen Sie als Zieladresse die IP-Adresse Ihres DNS-Servers fest.
Aktivieren Sie Gespiegelt, um den Eingabefilter automatisch zu erstellen.
Legen Sie die Protokolleinstellungen von Von diesem Port und Zu diesem Port für den Port fest, der auf Ihrem DNS-Server für die Datenübertragung eingerichtet ist. Es handelt sich normalerweise um Port 53.

Setzen Sie die Filteraktion auf Zulassen, um sicherzugehen, dass der DNS-Datenverkehr weitergeleitet und keine Sicherheit für dieser IP-Filterliste entsprechenden Datenverkehr ausgehandelt wird.

Vorsicht

Die Verwendung eines DNS-Namens anstelle einer IP-Adresse in der IP-Sicherheitsrichtlinie vereinfacht die Verwaltung, es sollte jedoch nur eine statische IP-Adresse des Computers (eine nicht automatisch vom DHCP-Dienst ausgegebene Adresse) verwendet werden, zu der der DNS-Name aufgelöst werden kann. Wenn z. B. ein Angreifer in den DNS-Server eindringt und den der IP-Adresse zugeordneten

DNS-Namen ändert, löst IPSec den Namen in eine andere IP-Adresse auf, was unsicheren Datenverkehr zur Folge hat.

Eigenschaften einer IP-Sicherheitsrichtlinie

IP-Sicherheitsrichtlinien können auf lokale Computer, Domänenmitglieder, Domänen, Organisationseinheiten oder ein beliebiges Gruppenrichtlinienobjekt in Active Directory angewendet werden. Grundlage für die IP-Sicherheitsrichtlinien Ihrer Organisation sollten die schriftlich festgehaltenen Leitlinien der Organisation für sichere Operationen sein. In den Richtlinien können mehrere Sicherheitsmaßnahmen gespeichert sein, die Regeln heißen, so dass eine Richtlinie auf mehrere Computer angewendet werden kann.

Es gibt zwei Speicherorte für IP-Sicherheitsrichtlinien:

Active Directory.

Lokal in der Registrierung für Einzelcomputer und solche, die nicht ständig zu einer vertrauenswürdigen Windows 2000-Domäne gehören, festgelegt. Ist der Computer zeitweise nicht an eine vertrauenswürdige Windows 2000-Domäne angeschlossen, werden die Richtlinieninformationen in der lokalen Registrierung zwischengespeichert. Weitere Informationen erhalten Sie unter Übersicht über Active Directory.

Windows enthält vordefinierte Richtlinien, die aktiviert oder Ihren Wünschen entsprechend geändert werden können; sie können auch als Vorlage für eigene Richtlinien dienen. Jede Richtlinie, die Sie festlegen, sollte für ein Szenario in Ihrem Sicherheitsplan gelten. Möglicherweise sind bestimmte Konfigurationseinstellungen notwendig, wenn Sie einem DHCP-Server, Domänennamensystem (DNS), WINS, Simple Network Management Protocol (SNMP) oder RAS-Server Richtlinien zuweisen.

Gruppenrichtlinie

IP-Sicherheitsrichtlinien, die einem Gruppenrichtlinienobjekt in Active Directory zugewiesen werden, werden Bestandteil der Gruppenrichtlinie und werden bei jedem Weiterleiten der Gruppenrichtlinien auf die beteiligten Computer übertragen. Weitere Informationen über die Gruppenrichtlinien erhalten Sie unter Übersicht über Gruppenrichtlinien.

Beim Zuweisen einer IP-Sicherheitsrichtlinie in Active Directory berücksichtigen Sie bitte Folgendes:

IP-Sicherheitsrichtlinien, die Domänenrichtlinien zugewiesen sind, setzen alle lokalen aktiven IP-Sicherheitsrichtlinien außer Kraft, wenn der Computer mit der Domäne verbunden ist.

IP-Sicherheitsrichtlinien, die einer Organisationseinheit zugewiesen sind, setzen IP-Sicherheitsrichtlinien außer Kraft, die den Domänenrichtlinien zugewiesen ist; dies gilt für alle Mitglieder dieser Organisationseinheit. Die der niedrigsten Organisationseinheit zugewiesenen IP-Sicherheitsrichtlinien setzen IP-

Sicherheitsrichtlinien außer Kraft, die einer höheren Organisationseinheit zugewiesen ist; dies gilt für alle Mitglieder dieser Organisationseinheit.

IP-Filterlisten

Eine IP-Filterliste löst Sicherheitsaushandlungen aus, die auf Übereinstimmung mit der Quelle, dem Ziel und der IP-Datenübertragungsart basieren. Mit diesem IP-Paketfiltertyp kann die Netzwerkadministration genau festlegen, welcher IP-Datenverkehr gesichert wird. Jede IP-Filterliste enthält einen oder mehrere Filter, mit denen die IP-Adressen und Datenverkehrstypen festgelegt werden. Eine einzelne IP-Filterliste kann für mehrere Szenarios der Datenübertragung verwendet werden.
Bei Verwendung von IPSec ist für jeden in der Filterliste enthaltenen Computer ein Eingabe- und Ausgabefilter erforderlich. Eingabefilter werden auf den eingehenden Datenverkehr angewendet, der empfangende Computer ist in der Lage, auf Anforderungen gesicherter Datenübertragung zu antworten oder den Datenübertragungsart auf Übereinstimmung mit der IP-Filterliste zu überprüfen. Ausgabefilter werden auf den vom Computer zu einem bestimmten Ziel gesendeten Datenverkehr angewendet, eine Sicherheitsaushandlung wird ausgelöst, die vor dem Senden der Daten ausgeführt wird. Im folgenden Beispiel soll ein gesicherter Datenaustausch zwischen Computer A und Computer B ausgeführt werden:
Die aktive IP-Sicherheitsrichtlinie auf Computer A muss einen Filter für alle nach Computer B ausgehenden Pakete haben. Quelle=A, Ziel=B.
Die aktive IP-Sicherheitsrichtlinie auf Computer A muss einen Filter für alle von Computer B eingehenden Pakete haben. Quelle=B, Ziel=A.
Jeder Peer muss außerdem den jeweiligen Umkehrfilter haben:
Die aktive IP-Sicherheitsrichtlinie auf Computer B muss einen Filter für alle von Computer A eingehenden Pakete haben. Quelle=A, Ziel=B.
Die aktive IP-Sicherheitsrichtlinie auf Computer B muss einen Filter für alle nach Computer A ausgehenden Pakete haben. Quelle=B, Ziel=A.

Filtereinstellungen

Mit jedem Filter wird festgelegt, wie ein bestimmter Bereich des ein- und ausgehenden Netzwerkdatenverkehrs gesichert wird. Für den gesamten Datenverkehr, auf den die zugeordnete Regel angewendet wird, muss ein Filter eingerichtet sein. Ein Filter enthält die folgenden Einstellungen:
Die Quell- und Zieladresse des IP-Pakets. Diese kann entweder auf einer weiterverzweigten Ebene mit einer IP-Adresse oder einem DNS-Namen oder mit Adressengruppen, Subnetzen oder Netzwerken konfiguriert werden.
Das Protokoll, mit dem das Paket übertragen wird. Standardmäßig werden alle Protokolle der TCP/IP-Protokollsuite angewendet. Der Filter kann jedoch im Bedarfsfall individuell auf Protokollebene, einschließlich benutzerdefinierter Protokolle, konfiguriert werden.

Der für TCP und UDP vorgesehene Quell- und Zielport des Protokolls. Standardmäßig können alle Ports verwendet werden, aber die Konfiguration bestimmter Ports ist möglich.
Weitere Informationen über das Konfigurieren von IP-Filterlisten finden Sie unter Hinzufügen und Bearbeiten von IP-Filterlisten.

Für bestimmte Datenübertragungstypen, wie z. B. SNMP oder Sicherheitsgateways, können spezielle Filter erforderlich sein. Weitere Informationen erhalten Sie unter Besondere Vorüberlegungen zur IP-Sicherheit.

Filteraktionen

In einer Filteraktion werden die Sicherheitsanforderungen für die Datenübertragung definiert. Eine Filteraktion kann folgendermaßen konfiguriert werden:
Bereitstellen der Funktionen einer Passthrough-Richtlinie ("Zulassen"). Die Aushandlung sicherer Kommunikation ist auf diese Weise nicht möglich. IPSec ignoriert in diesem Fall einfach die Datenübertragung. Diese Funktionen sind bei Computern, wie z. B. WebTV-Servern, vorteilhaft, die ausschließlich Broadcastinformationen übertragen, ohne dass ein besonderer Schutz erforderlich ist. Begrenzen Sie bei Verwendung dieses Filteraktionstyps den Geltungsbereich der IP-Filterliste auf ein Minimum, um die Erfordernis der Durchführung gesicherten Datenverkehrs zu umgehen.

Datenverkehr sperren ("Sperren"). Die Datenübertragung von einem nicht autorisierten Computer wird gestoppt. Beim Sperren einer Filteraktion sollte eine IP-Filterliste möglichst geringen Umfangs verwendet werden, um berechtigte Computer nicht von der Kommunikation auszusperren.

Aktivieren Sie die Kommunikation mit nicht IPSec-aktivierten Computern. (Verwenden Sie die Optionen"Unsichere Kommunikation zulassen, aber immer mit IPSec antworten" und "Unsichere Kommunikation mit Computern zulassen, die IPSec nicht unterstützen".) Bei dieser Filteraktion wird ggf.auf die ungesicherte Kommunikation zurückgegriffen. Auch in diesem Fall sollte der Geltungsbereich der IP-Filterliste auf ein Minimum reduziert werden. Ansonsten kann ein Fehlschlagen einer Sicherheitsaushandlung zur Folge haben, dass die Regel, in der diese Filteraktion aktiv ist, den betroffenen Datenverkehr auch ungesichert ausführt. Wenn der Schutz vor Angriffen ein wichtiger Faktor ist, sollte das Deaktivieren dieser Einstellungen in Betracht gezogen werden. Die Datenübertragung mit Computern, die IPSec beispielsweise aufgrund veralteter Betriebssysteme nicht initiieren können, wird möglicherweise gesperrt.

"Sitzungsschlüssel für Perfect Forward Secrecy (PFS) aktivieren." Legt fest, wie ein neuer Schlüssel erstellt wird. Das Aktivieren von PFS stellt sicher, dass ein zum Schutz einer Übertragung verwendeter Schlüssel nicht zur Erstellung zusätzlicher Schlüssel verwendet werden kann. Darüber hinaus kann das Schlüsselmaterial für diesen Schlüssel nicht zur Erstellung neuer Schlüssel verwendet werden. Sitzungsschlüssel für PFS erfordern keine erneute Authentifizierung und beanspruchen daher weniger Ressourcen als Hauptschlüssel für PFS. Wenn Sitzungsschlüssel für PFS aktiviert ist, wird ein neuer Schlüsselaustausch ausgeführt, um vor dem Erstellen eines neuen Sitzungsschlüssels neues Schlüsselmaterial anzusammeln.

Sicherheitserfordernisse festlegen ("Diese Sicherheitseinstellungen verwenden"). Die Liste der auszuhandelnden Sicherheitserfordernisse wird als Sicherheitsmethoden bezeichnet. In jeder Methode sind die auszuhandelnden Algorithmen, Sicherheitsprotokolle und die Einsatzdauer der Schlüssel festgelegt.

IP-Sicherheitsmethoden

Durch jede Sicherheitsmethode werden die Sicherheitsanforderungen jeder Kommunikation festgelegt, auf die die verknüpfte Regel angewendet wird . Das Erstellen mehrerer Sicherheitsmethoden erhöht die Chance, dass zwei Computer über eine gemeinsame Sicherheitsmethode verfügen.
Der Dienst ISAKMP/Oakley liest die Liste der Sicherheitsmethoden in absteigender Reihenfolge und tauscht Aushandlungsnachrichten mit anderen Peers so lange aus, bis eine gemeinsame Methode gefunden wurde.

Vordefinierte IP-Sicherheitsmethoden

Hoch. Verwendet Encapsulating Security Payload (ESP), um Vertraulichkeit (Datenverschlüsselung), Authentifizierung, Anti-Replay und Integrität zu bieten, wobei diese für den Fall angepasst werden, dass hohe Sicherheitsstufen erforderlich sind. ESP bietet keine Integrität für IP-Header (Adressierung). Möchten Sie Daten- und Adressierungsschutz, können Sie eine benutzerdefinierte Sicherheitsmethode erstellen. Möchten Sie keine Verschlüsselung, verwenden Sie Mittel.
Mittel. Verwendet das Protokoll Authentication Header (AH), um Integrität, Anti-Replay, und Authentifizierung zu bieten. Dies ist dann geeignet, wenn Ihr Sicherheitsplan Standardsicherheitsstufen erfordert. AH bietet Integrität für IP-Header und Daten, verschlüsselt die Daten aber nicht.

Benutzerdefinierte IP-Sicherheitsmethoden

Profis können benutzerdefinierte Sicherheitsmethoden festlegen, wenn Verschlüsselung und Adressierungsintegrität, stärkere Algorithmen oder Schlüsselgültigkeitsdauer erforderlich sind:

Sicherheitsprotokolle

AH und ESP können in einer benutzerdefinierten Sicherheitsmethode aktiviert sein, wenn Sie IP-Header-Integrität und Datenverschlüsselung möchten. Möchten Sie beides aktivieren, müssen Sie keinen zweiten Integritätsalgorithmus für ESP erstellen; der für AH ausgewählte Algorithmus bietet Integrität.

Integrität

Nachrichtendigest 5 (MD5), der einen 128-Bit-Schlüssel produziert.
Sicherer Hashalgorithmus (SHA), durch den ein 160-Bit-Schlüssel erstellt wird. Größere Schlüssellängen bieten höheren Schutz, so dass SHA sehr sicher sein kann.

Vertraulichkeit

3DES ist die sicherste DES-Kombination und deshalb etwas langsamer in der Leistung. 3DES führt jeden Block dreimal aus und verwendet dabei jedes Mal einen anderen einmaligen Schlüssel.
DES sollte eingesetzt werden, wenn die hohe Sicherheit und die Anforderungen von 3DES nicht notwendig sind, außerdem aus Gründen der Interoperabilität. DES benötigt nur 56 Bit Schlüsselmaterial.

Schlüsselgültigkeitsdauern

Durch Schlüsselgültigkeitsdauern wird festgelegt, wann - aber nicht wie - ein Schlüssel generiert wird. Sie können die Gültigkeitsdauer in Kilobyte, Sekunden oder beiden Einheiten festlegen. Dauert die Kommunikation beispielsweise 100,000 Sekunden und Sie haben die Schlüsselgültigkeitsdauer auf 1000 Sekunden festgelegt, werden zehn Schlüssel zum Vervollständigen der Übertragung generiert. Dadurch wird sichergestellt, dass wenn Personen von außen in eine Kommunikation "einbrechen", sie nicht die gesamte Kommunikation verfolgen können. Automatische Schlüsselneuerstellung wird zur Verfügung gestellt; die Konfiguration ist optional. Beachten Sie, dass nach jedem Ablaufen der Schlüsselgültigkeitsdauer zusätzlich zur Schlüsselerneuerung und -neuerstellung auch SA neu ausgehandelt wird.
Interoperabilität von Verschlüsselungseinstellungen
Wenn Sie IPSec für die Vertraulichkeit von Daten zwischen einem Windows 2000-Computer mit High Encryption Pack und einem anderen Computer ohne 3DES einsetzen, ist DES als Sicherheitsmaßnahme zwingend erforderlich. Andernfalls erlangt der Computer, mit dem Sie zu kommunizieren versuchen, möglicherweise keine Sicherheitsübereinstimmung mit Ihrem Computer. Falls keine Vertraulichkeit der Daten erforderlich ist, können Sie das ESP-Format mit einem Algorithmus für die Integrität auswählen und die Verschlüsselung Keine festlegen. Alternativ verwenden Sie ein AH-Format mit einem Integritätsalgorithmus.
Weitere Informationen über das Konfigurieren von Sicherheitsmethoden finden Sie unter So fügen Sie Sicherheitsmethoden hinzu oder bearbeiten diese.

Schlüsselaustausch

Die klaren Vorzüge von Schlüsseln, die die Schlüsselaustauschphase schützen, werden durch die folgenden Funktionen erweitert:

Schlüsselgültigkeitsdauer

Einstellungen hinsichtlich der Einsatzdauer, wann ein neuer Schlüssel erstellt wird. Wenn die Schlüsselgültigkeitsdauer erreicht ist, wird auch die zugehörige Sicherheitszuordnung neu ausgehandelt. Der Vorgang, neue Schlüssel in bestimmten Intervallen zu erstellen, wird als dynamischer Schlüssel oder Schlüsselneuerstellung bezeichnet. Die Gültigkeitsdauer ermöglicht die erzwungene Erstellung neuer Schlüssel (Schlüsselneuerstellung) nach einem bestimmten Intervall. Dauert eine Kommunikation beispielsweise 100 Minuten und beträgt die Schlüsselgültigkeitsdauer zehn Minuten, müssen während des Austausches alle zehn Minuten, also insgesamt zehn Schlüssel erstellt werden. Die Verwendung mehrerer Schlüssel stellt sicher, dass die gesamte Kommunikation nicht offengelegt wird, selbst wenn es ein Angreifer schaffen sollte, den Schlüssel eines Teiles der Kommunikation zu erhalten. Automatische Schlüsselneuerstellung wird standardmäßig zur Verfügung gestellt. Profis können diese Standards überschreiben und innerhalb von Minuten eine Hauptschlüsselgültigkeitsdauer nach Sitzungsschlüssel für Perfect Forward Secrecy erstellen.

Beim Einstellen sehr unterschiedlicher Schlüsselgültigkeitsdauern sollte äußerst vorsichtig vorgegangen werden, da diese auch die Gültigkeitsdauer der Sicherheitszuordnung festlegen. Wird beispielsweise eine Gültigkeitsdauer für den

Hauptschlüssel von acht Stunden (480 Minuten) und eine für den Sitzungsschlüssel (bei einer Filteraktion festgelegt) von zwei Stunden eingestellt, ist eine IPSec-Sicherheitszuordnung für fast zwei Stunden aktiv, nachdem die ISAKMP-Sicherheitszuordnung abgelaufen ist. Dies tritt möglicherweise auf, wenn eine neue IPSec-Sicherheitszuordnung direkt erstellt wird, bevor die ISAKMP-Sicherheitszuordnung abläuft.

Limit für den Sitzungsschlüssel

Wiederholte Schlüsselneuerstellungen desselben Hauptschlüssels führen möglicherweise zu einer Gefährdung des Schlüssels. Jan an Computer A sendet beispielsweise eine Nachricht an Tanja an Computer B, und einige Minuten später sendet er eine weitere Nachricht an Tanja; dasselbe Hauptschlüsselmaterial kann erneut verwendet werden, da zuvor mit diesem Computer eine Sicherheitszuordnung eingerichtet worden ist. Wenn Sie die Häufigkeit der Wiederverwendung begrenzen möchten, können Profis ein Limit für den Sitzungsschlüssel angeben.
Beachten Sie jedoch bei der Aktivierung von Perfect Forward Secrecy für den Hauptschlüssel, dass das Limit für den Sitzungsschlüssel ignoriert wird; PFS erzwingt jedes Mal eine Schlüsselneuerstellung. Beispielsweise entspricht die Aktivierung eines Hauptschlüssels für Perfect Forward Secrecy dem Festlegen eines auf Eins (1) gesetzten Sitzungsschlüssels.
Beachten Sie, dass beim Festlegen einer Gültigkeitsdauer für den Haupt- und Sitzungsschlüssel in Minuten das jeweils zuerst erreichte Intervall einen neuen Schlüssel auslöst.

Hauptschlüssel für Perfect Forward Secrecy (PFS)

Legt fest, wie ein neuer Schlüssel erstellt wird. Das Aktivieren von PFS stellt sicher, dass ein zum Schutz einer Übertragung verwendeter Schlüssel in keiner Phase zur Erstellung zusätzlicher Schlüssel verwendet werden kann. Darüber hinaus kann das Schlüsselmaterial für diesen Schlüssel nicht zur Erstellung neuer Schlüssel verwendet werden.
Hauptschlüssel für PFS sollten nur mit Bedacht verwendet werden, da erneute Authentifizierungen nötig werden. Dies kann zu einem zusätzlichen Verwaltungsaufwand für Domänencontroller im Netzwerk führen. Es ist nicht notwendig, dass dieser auf beiden Computern aktiviert ist.
Weitere Informationen zur Konfiguration von Einstellungen und Methoden zum Schlüsselaustausch finden Sie unter So konfigurieren Sie den Schlüsselaustausch und So erstellen Sie Schlüsselaustauschmethoden.

Methoden für den Schlüsselaustausch

Neben den Eigenschaften der Schüssel können fortgeschrittene Benutzer die Sicherheitsmethoden für Phase I (Hauptmodus) der IKE-Aushandlung festlegen. In der Regel sollten Sie die Standardwerte für alle IKE-Einstellungen (PFS, Schlüsselgültigkeitsdauer) und die Sicherheitsmethoden beibehalten, so dass eine unnötige Mehrbelastung vermieden wird. Dadurch wird eine standardmäßige (mittlere) Sicherheitsstufe gewährleistet. Sieht Ihr Sicherheitsplan eine höhere Sicherheitsstufe vor, können Sie ggf. die Standardsicherheitsmethoden ändern.
Sie können angeben, welche Algorithmen für die Integrität und Vertraulichkeit (optional) verwendet werden sollen. Dieselben Algorithmen für Phase II-

Sicherheitsmethoden stehen hier zur Verfügung: MD5 und SHA für die Integrität, DES und 3DES für die Vertraulichkeit.

Diffie-Hellman-Gruppen

Diffie-Hellman-Gruppen werden zur Festlegung der Länge von Basisprimzahlen verwendet, die während des Schlüsselaustausches verwendet werden. Die klaren Vorzüge von abgeleiteten Schlüsseln hängt teilweise von der Stärke der Diffie-Hellman-Gruppe ab, auf der die Primzahlen basieren:
Gruppe 2 (Mittel) ist dabei leistungsstärker als Gruppe 1 (Niedrig). Gruppe 1 bietet 768 Bit Schlüsselmaterial, Gruppe 2 dagegen 1.024 Bit. Stimmen die Gruppen auf den Peers nicht überein, schlägt die Aushandlung fehl. Die Gruppen können nicht während der Aushandlung gewechselt werden.

Eine höhere Gruppe führt zu Ergebnissen mit höherer Entropie und daher zu einem sichereren Schlüssel, der schwieriger zu dechiffrieren ist.
Die Diffie-Hellman-Gruppe wird als Bestandteil der Phase-I(Hauptmodus)-Einstellungen für den Schlüsselaustausch konfiguriert. Diese Gruppe ist einer der Hauptschlüssel. Neue Schlüssel, die Sie während der Datenschutzphase II (schneller Modus) erzeugen, werden vom Diffie-Hellman-Phase-I-Hauptschlüssel abgeleitet, sofern Sie nicht Phase-II-Perfect Forward Secrecy einsetzen.
Weitere Informationen zur Konfiguration von Einstellungen und Methoden zum Schlüsselaustausch finden Sie unter So konfigurieren Sie den Schlüsselaustausch und So erstellen Sie Schlüsselaustauschmethoden.

Domänen, Peer-to-Peer: IPSec

Um Sicherheit für Gruppen bereitzustellen, in denen oft ein Austausch hochsensibler Informationen stattfand, musste das Intranet häufig segmentiert werden. Durch das Anordnen von Computergruppen auf verschiedenen physischen Segmenten konnten Sicherheitsverletzungen verhindert werden. IPSec stellt darüber hinaus Sicherheit für Computergruppen bereit, die sich in demselben physischen Intranet befinden.

Für jeden Computer ist ein Computerkonto in einer Active Directory-Domäne oder einem -Objekt eingerichtet. Aus Sicherheitsgründen sind die Computer in Active Directory-Organisationseinheiten gruppiert. Dies ermöglicht die passende Zuordnung von auf der Funktionalität des betreffenden Computers basierenden IP-Richtlinien:
Server, auf denen hochsensible Informationen gespeichert und ausgetauscht werden, gehören zur Organisationseinheit der Server mit höchster Sicherheit.
Server, auf denen die ungesicherte Datenübertragung mit nicht IPSec-fähigen Computern möglich ist, gehören zur Organisationseinheit der sicheren Server.
Clients, die in der Lage sein müssen, auf Anforderungen sicherer Datenübertragung entsprechend zu antworten, gehören zur Gruppe der sicheren Computer,
Clients, die den sicheren Servern nicht antworten müssen, gehören zur Standardcomputergruppe.

Beim Gruppieren von Computern in Organisationseinheiten kann die Zuweisung der IP-Richtlinien auf die Computer beschränkt werden, die IPSec benötigen. Dies ermöglicht auch die Zuordnung der entsprechenden Sicherheitsstufe und hilft, zusätzlichen Sicherheitsaufwand zu vermeiden. In diesem Szenario werden die IP-Richtlinien für alle Computer in Active Directory gespeichert.

Zwischen den Clients und dem Domänencontroller ist keine hohe Sicherheit erforderlich: Der mit dem Kerberos-Protokoll ausgeführte Datenaustausch zwischen den Clients und dem Domänencontroller ist bereits verschlüsselt, und die IPSec-Richtlinienübertragung von Active Directory zu den Mitgliedscomputern wird über die Windows LDAP-Sicherheit geschützt.

IPSec sollte in diesem Fall mit der durch Zugriffssteuerungsmaßnahmen bereitgestellten Sicherheit kombiniert werden. Benutzerberechtigungen sind weiterhin notwendig, um die auf den Servern mit höchster oder sehr hoher Sicherheit freigegebenen Dateien vor unberechtigtem Zugriff zu schützen. IPSec sichert den Datenverkehr auf Netzwerkebene, so dass Angreifer die Daten nicht lesen oder ändern können.

Vordefinierte Konfigurationen

Windows 2000 enthält eine Reihe vordefinierter IPSec-Konfigurationen. Standardmäßig sind alle vordefinierten Richtlinien für Windows 2000-Domänenmitglieder konzipiert. Im folgenden werden die vordefinierten Richtlinien von Windows 2000 beschrieben. Die vordefinierten Richtlinien, die Filterlisten und die Filteraktionen auf dem lokalen Computer und in Active Directory sind nicht für den unmittelbaren Einsatz konzipiert. Mit diesen Elementen sollen lediglich die Unterschiede in den Verhaltensweisen bei verschiedenen Richtlinieneinstellungen dargestellt werden.

Computer: Client (Nur Antwort)

Diese Richtlinie dient für Computer, bei denen eine sichere Kommunikation in der Regel nicht erforderlich ist. Beispielsweise ist die Verwendung von IPSec auf Intranetclients nicht erforderlich, es sei denn, diese wird von einem anderen Computer angefordert. Diese Richtlinie ermöglicht es dem betreffenden Computer, auf Anforderungen gesicherter Datenübertragung entsprechend zu antworten. Die Richtlinie enthält eine Standardantwortregel, die die Aushandlung mit IPSec-anfordernden Computern ermöglicht. Sicherheit wird entsprechend der Anforderung auf den Datenverkehr der betreffenden Protokolle und Ports begrenzt.

Sichere Server: Server (Sicherheit anfordern)

Diese Richtlinie dient für Computer, bei denen eine sichere Kommunikation in der Regel erforderlich ist, beispielsweise für Server, die zur Übertragung vertraulicher Daten eingesetzt werden. Bei dieser Richtlinie wird ungesicherter Datenverkehr akzeptiert. Der Computer richtet jedoch ständig Sicherheitsanforderungen an den Sender und versucht so, weitere Datenübertragungen zu sichern. Diese Richtlinie ermöglicht die vollständige ungesicherte Datenübertragung, wenn der andere Computer nicht IPSec-aktiviert ist.
Server mit höchster Sicherheit: Sicherer Server (Sicherheit erforderlich)
Diese Richtlinie gilt für Computer, bei denen eine sichere Kommunikation stets erforderlich ist, beispielsweise für Serer, die zur Übertragung hochsensibler Daten eingesetzt werden. Bei dieser Richtlinie wird ungesicherter eingehender Datenverkehr akzeptiert; ausgehender Datenverkehr wird dagegen immer gesichert.

Remoteübertragung: IPSec

Sichere Remoteübertragung wird durch Kombinieren von IPSec mit dem Layer 2 Tunneling-Protokoll (L2TP) gewährleistet. L2TP wird zum Erstellen eines Tunnels verwendet, durch den die Daten übertragen werden, während die Datensicherung über IPSec erfolgt.

Clients mit wechselnden Standorten

Das Sichern der Datenübertragung zwischen Remoteclients und dem Unternehmensnetzwerk ist ein häufig auftretendes Erfordernis. Beispielsweise muss ein häufig im Außendienst tätiger Verkaufsberater oder ein von zu Hause arbeitender Angestellter remote auf das Netzwerk zugreifen können.

Zweigstellen

Große Unternehmen haben häufig mehrere Standorte, die untereinander kommunizieren müssen, z. B. eine Unternehmenszentrale in New York und ein Verkaufsbüro in Washington. Wie im vorhergehenden Szenario wird L2TP mit IPSec kombiniert, um den Tunnel bereitzustellen und die zwischen den Standorten übertragenen Daten zu schützen.

Sichern der Remoteübertragung

Anstelle der Konfiguration von IP-Sicherheitsrichtlinien ist bei diesen Remoteübertragungsszenarios die Konfiguration der L2TP-Sicherheitseigenschaften von Windows 2000 erforderlich.
Folgende Vorgänge werden bei der Konfiguration von L2TP zusammen mit IPSec ausgeführt:

Die erforderlichen IP-Filter und Filteraktionslisten werden dynamisch im IP-Sicherheitsrichtlinien-Agents während der Dauer der Verbindung angepasst.
Die Authentifizierung wird durch L2TP bestimmt. Hierbei wird ein öffentliches Schlüsselzertifikat sowie der zugehörige private Schlüssel für einen Computer benötigt.

Die Standardeinstellungen für den Schlüsselaustausch sind gültig.

Der Sicherheitsgrad des IP-Protokolls während der Verbindungsdauer hängt von der L2TP-Sicherheitskonfiguration ab:
Keine Verschlüsselung. IPSec fordert weiterhin ein Zertifikat an und ist für die Aushandlung von AH zuständig.
Optionale Verschlüsselung. Wenn der andere Computer gesicherte Datenübertragung anfordert oder benötigt, bietet IPSec Sicherheitsstufen von ESP/3DES bis AH/MD5.
Der Sitzungsschlüssel Perfect Forward Secrecy wird erst aktiviert, wenn der Computer dies anfordert.
Auf die ungesicherte Datenübertragung kann zurückgegriffen werden.

Angeforderte Verschlüsselung. Der Computer erfordert sichere Datenübertragung. Der Umfang der angebotenen Sicherheit entspricht dem mit der optionalen Verschlüsselung gewährleisteten Sicherheitsumfang, mit der Ausnahme, dass nicht auf die ungesicherte Datenübertragung zurückgegriffen werden kann.

Empfehlungen

Planen einer effizienten Implementierung
Ermitteln Sie die verschiedenen Arten von Informationen, die über das Netzwerk Ihres Unternehmens übertragen werden. Handelt es sich um hochsensible finanzielle Daten, geschützte Informationen oder E-Mail? Von Abteilung zu Abteilung können, je nach Aufgabenbereich, unterschiedliche Sicherheitsanforderungen an die Datenvertraulichkeit gestellt werden.

Legen Sie fest, wo die Informationen gespeichert werden sollen, wie sie durch das Netzwerk geroutet und von welchen Computern darauf zugegriffen werden soll. Auf diese Weise werden vor der Implementierung eines Netzwerks Informationen über Geschwindigkeit, Kapazität und Auslastung bereitgestellt, mit denen Angaben zur Leistungsoptimierung erstellt werden können.

Beurteilen Sie die Anfälligkeit gegenüber Netzwerkattacken.

Entwerfen und dokumentieren Sie einen unternehmensweiten Netzwerksicherheitsplan. Berücksichtigen Sie die Sicherheitsumgebung von Windows unter Einbeziehung des Active Directory-Modells und der Gruppenrichtlinien-Sicherheit. Weitere Informationen erhalten Sie unter Übersicht über Active Directory.

Folgendes sollte bei der Planung berücksichtigt werden:

- Wofür soll Sicherheit implementiert werden? Soll Sicherheit für den gesamten
- Datenverkehr zwischen bestimmten Computern, allen Computern oder nur zwischen bestimmten Protokollen und Ports eingerichtet werden?
- Wie soll Sicherheit implementiert werden? Wie hoch soll der für den Datenverkehr eingerichtete Integritäts- bzw. Vertraulichkeitsgrad bei Verwendung dieser Sicherheitsoptionen sein?
- Wo soll Sicherheit implementiert werden? Sollen alle RAS-Verbindungen oder das gesamte LAN-Netzwerk einbezogen werden?
- Wer verwaltet die entsprechenden Richtlinien? Wird mit der Richtlinienverwaltung die Domänen-, die Serveradministration oder die Administration des lokalen Computers beauftragt?
- Können die Verschlüsselungseinstellungen bei allen relevanten Computern eingesetzt werden? Erfolgt der Datenzugriff sowohl über Computer mit starker Kryptografie (3DES-Verschlüsselung) als auch über Computer mit Standardkryptografie?

Des Weiteren sollte Folgendes berücksichtigt werden:

- Entwerfen, Erstellen und Testen der IPSec-Richtlinien zum Ermitteln und Definieren der geeigneten Richtlinien und -strukturen. Während der Test- und Einsatzszenarios sollte eine dem üblichen Maß entsprechende Arbeitsauslastung

gewährleistet sein, um realistische Angaben zu erhalten. Um zu Beginn der Testphase die Paketinhalte mit dem Netzwerkmonitor oder einem Sniffer anzuzeigen, verwenden Sie die Mittlere Sicherheitsstufe oder eine angepasste, auf AH gesetzte Sicherheitsmethode, da die Paketanzeige bei Verwendung von High oder ESP nicht möglich ist.

?? Reduzieren Sie den administrativen Aufwand, indem Sie nach Möglichkeit vordefinierte Richtlinien, Regeln und Filteraktionen verwenden. Diese können als Vorlage verwendet und jederzeit aktiviert und modifiziert werden.

Erläuterung der IPSec Statisktiken von IPSECMON

IPSec Statistik

Aktive Zuordnungen

Die Anzahl aktiver Sicherheitszuordnungen auf diesem Computer

Gesendete vertrauliche Bytes

Die Gesamtanzahl an Bytes, die mit ESP-Vertraulichkeit gesendet wurden. Hierdurch wird angezeigt, dass die Pakete mit Hilfe des Sicherheitsprotokolls Encapsulating Security Payload (ESP), Dezimal-ID 50, gesendet wurden.

Empfangene vertrauliche Bytes

Die Gesamtanzahl an Bytes, die mit ESP-Vertraulichkeit empfangen wurden. Hierdurch wird angezeigt, dass die Pakete mit Hilfe des Sicherheitsprotokolls Encapsulating Security Payload (ESP), Dezimal-ID 50, gesendet wurden.

Gesendete authentifizierte Bytes

Die Gesamtanzahl an Bytes, die mit aktivierter Authentifizierung gesendet wurden.

Empfangene authentifizierte Bytes

Die Gesamtanzahl an Bytes, die mit aktivierter Authentifizierung empfangen wurden.

Fehlerhafte SPI-Pakete

Die Gesamtanzahl der Pakete, für die der Sicherheitsparameterindex (Security Parameters Index, SPI) ungültig war. Dies kann bedeuten, dass die Sicherheitszuordnung (Security Association, SA) abgelaufen oder nicht mehr gültig ist.
SPI ist ein eindeutiger, kennzeichnender Wert in der Sicherheitszuordnung, der es dem empfangenden Computer ermöglicht, die Sicherheitszuordnung auszuwählen, mit der ein Paket verarbeitet wird.

Nicht entschlüsselte Pakete

Die Gesamtanzahl der Pakete, die der empfangende IPSec-Treiber nicht entschlüsseln konnte. Dies kann bedeuten, dass die Sicherheitszuordnung

abgelaufen oder nicht mehr gültig ist oder die Authentifizierung oder Integritätsprüfung fehlgeschlagen ist.

Nicht authentifizierte Pakete

Die Gesamtanzahl der Pakete, die vom IPSec-Treiber nicht erfolgreich authentifiziert wurden. Dies kann bedeuten, dass die Sicherheitszuordnung abgelaufen oder nicht mehr gültig ist. Die Informationen in der Sicherheitszuordnung sind erforderlich, damit der IPSec-Treiber die Pakete verarbeiten kann. Es kann aber auch bedeuten, dass die Authentifizierungseinstellungen der beiden Computer nicht kompatibel sind. Prüfen Sie, ob für beide Computer dieselbe Authentifizierungsmethode angegeben ist.

Schlüsselerweiterungen

Die Gesamtanzahl der Schlüssel, die ISAKMP (der ISAKMP/Oakley-Mechanismus) an den IPSec-Treiber gesendet hat. Das bedeutet, dass die ISAKMP-Phase-II-Sicherheitszuordnungen erfolgreich ausgehandelt wurden.

ISAKMP/Oakley-Statistik

Oakley-Hauptmodi

Die Gesamtanzahl erfolgreicher Sicherheitszuordnungen, die während ISAKMP Phase I eingerichtet wurden. Das bedeutet, der Austausch der Schlüsselinformationen war erfolgreich: Identitäten wurden authentifiziert und gemeinsames Schlüsselmaterial eingerichtet.

Oakley-Schnellmodi

Die Gesamtanzahl erfolgreicher Sicherheitszuordnungen, die während ISAKMP Phase II eingerichtet wurden. Dies bedeutet, dass die Aushandlung der Schutzdienste während der Datenübertragung erfolgreich war.

Ladbare Zuordnungen

Die Gesamtanzahl der ISAKMP-Phase-II Aushandlungen, die dazu führten, dass die Computer sich nur auf eine Klartextdatenübertragung geeinigt haben (keine Verschlüsselung oder Signierung der Pakete).

Authentifizierungsfehler

Gesamtanzahl der fehlgeschlagenen Authentifizierungen der Computeridentitäten. Prüfen Sie, ob die Einstellungen der Authentifizierungsmethode für alle Computer kompatibel ist. Dies kann auch bedeuten, dass die Sicherheitszuordnung abgelaufen ist.