Contents

Aktivieren von vordefinierten Eingangsregeln

Aktivieren von vordefinierten Ausgangsregeln

Ausschließen von ICMP aus der Authentifizierung

Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne

Ändern der GPO-Filter

Öffnen von IP-Sicherheitsrichtlinien

Öffnen Sie die Gruppenrichtlinien

Öffnen der Gruppenrichtlinie

Öffnen der Windows-Firewall

Einschränken des Serverzugriffs

Aktivieren der Windows-Firewall

Überprüfen des Netzwerkdatenverkehrs

Windows Defender-Firewall mit erweiterter Sicherheit

20.11.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Dies ist eine Übersicht über die Windows Defender-Firewall mit erweiterter Sicherheit (wfas) und IPSec-Features (Internet Protocol Security).

Featurebeschreibung

Die Windows Defender-Firewall mit erweiterter Sicherheit ist ein wichtiger Bestandteileines mehrstufigen Sicherheitsmodells. Durch die Bereitstellung einer hostbasierten, bidirektionalen Netzwerkdaten Verkehrs Filterung für ein Gerät blockiert die Windows Defender-Firewall den unbefugten Netzwerkdatenverkehr, der in das oder aus dem lokalen Gerät fließt. Die Windows Defender-Firewall funktioniert auch mit der Netzwerkerkennung, damit Sie Sicherheitseinstellungen anwenden kann, die für die Typen von Netzwerken geeignet sind, mit denen das Gerät verbunden ist. Die Windows Defender-Firewall und die IPSec-Konfigurationseinstellungen (Internet Protocol Security) sind in eine einzige Microsoft Management Console (MMC) mit dem Namen Windows Defender Firewall integriert, sodass die Windows Defender-Firewall auch ein wichtiger Bestandteil des Netzwerks ist Isolierungs Strategie

Praktische Anwendungsfälle

Um die Herausforderungen ihrer organisatorischen Netzwerksicherheit zu beheben, bietet die Windows Defender-Firewall die folgenden Vorteile:

- **Verringert das Risiko von Bedrohungen durch Netzwerksicherheit.** Die Windows Defender-Firewall reduziert die Angriffsfläche eines Geräts und stellt eine zusätzliche Ebene für das mehrstufige Verteidigungsmodell bereit. Durch das Verringern der Angriffsfläche eines Geräts wird die Verwaltbarkeit erhöht und die Wahrscheinlichkeit eines erfolgreichen Angriffs verringert.
- **Schützt vertrauliche Daten und geistiges Eigentum.** Mit der Integration in IPSec bietet die Windows Defender-Firewall eine einfache Möglichkeit zum Erzwingen einer authentifizierten End-to-End-Netzwerkkommunikation. Es bietet skalierbaren, mehrstufigen Zugriff auf vertrauenswürdige Netzwerkressourcen, hilft, die Integrität der Daten zu erzwingen, und hilft optional, die Vertraulichkeit der Daten zu schützen.
- **Erweitert den Wert vorhandener Anlagen.** Da es sich bei der Windows Defender-Firewall um eine hostbasierte Firewall handelt, die im Betriebssystem enthalten ist, ist keine zusätzliche Hardware oder Software erforderlich. Die Windows Defender-Firewall dient auch dazu, vorhandene nicht von Microsoft bereitgestellten Netzwerk Sicherheitslösungen mithilfe einer dokumentierten API (Application Programming Interface) zu ergänzen.

Inhalt dieses Abschnitts

THEMA	BESCHREIBUNG

THEMA	BESCHREIBUNG
Isolieren von Microsoft Store-Apps in Ihrem Netzwerk	Sie können Ihre Windows Defender-Firewall-Konfiguration anpassen, um den Netzwerkzugriff von Microsoft Store-Apps zu isolieren, die auf Geräten ausgeführt werden.
Sichern von End-to-End-IPSec-Verbindungen mithilfe von IKEv2	Sie können IKEv2 verwenden, um Ihre End-to-End-IPSec-Verbindungen zu schützen.
Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell	Erfahren Sie mehr über die Verwendung von Windows PowerShell zum Verwalten der Windows Defender-Firewall.
Windows Defender-Firewall mit erweitertem Sicherheits Design-Leitfaden	Erfahren Sie, wie Sie ein Design für die Bereitstellung der Windows Defender-Firewall mit erweiterter Sicherheit erstellen.
Windows Defender-Firewall mit erweitertem Sicherheits Bereitstellungshandbuch	Erfahren Sie, wie Sie die Windows Defender-Firewall mit erweiterter Sicherheit bereitstellen.

Isolieren von Microsoft Store-Apps in Ihrem Netzwerk

07.08.2019 • 11 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie Ihrem Netzwerk neue Geräte hinzufügen, möchten Sie möglicherweise Ihre Windows Defender-Firewall mit erweiterter Sicherheitskonfiguration anpassen, um den Netzwerkzugriff der neuen Microsoft Store-Apps zu isolieren, die auf diesen Geräten ausgeführt werden. Entwickler, die Microsoft Store-Apps erstellen, können bestimmte App-Funktionen deklarieren, die verschiedene Klassen des Netzwerkzugriffs ermöglichen. Ein Entwickler kann entscheiden, welche Art von Netzwerkzugriff für die APP erforderlich ist, und diese Funktion für die APP konfigurieren. Wenn die APP auf einem Gerät installiert ist, werden die entsprechenden Firewallregeln automatisch erstellt, um den Zugriff zu ermöglichen. Sie können dann die Firewall-Konfiguration so anpassen, dass dieser Zugriff weiter optimiert wird, wenn Sie mehr Kontrolle über den Netzwerkzugriff für die APP wünschen.

Beispielsweise kann ein Entwickler beschließen, dass seine app nur mit vertrauenswürdigen lokalen Netzwerken (wie zu Hause oder in der Arbeit) und nicht mit dem Internet verbunden werden soll. Auf diese Weise können Entwickler den Umfang des Netzwerkzugriffs für Ihre APP definieren. Diese Netzwerkisolierung verhindert, dass eine APP auf ein Netzwerk und einen Verbindungstyp (eingehend oder ausgehend) zugreift, wenn die Verbindung nicht für die APP konfiguriert wurde. Dann kann der Netzwerkadministrator die Firewall so anpassen, dass die Ressourcen, auf die die App zugreifen kann, weiter eingeschränkt werden.

Die Möglichkeit, diese Netzwerkgrenzen festzulegen und zu erzwingen, stellt sicher, dass apps, die kompromittiert werden, nur auf Netzwerke zugreifen können, in denen Ihnen explizit Zugriff gewährt wurde. Dadurch wird der Umfang ihrer Auswirkungen auf andere apps, das Gerät und das Netzwerk erheblich reduziert. Darüber hinaus können apps isoliert und vor böswilligem Zugriff aus dem Netzwerk geschützt werden.

Beim Erstellen neuer Microsoft Store-Apps kann ein Entwickler die folgenden Netzwerkfunktionen für seine app definieren:

- **Home\Work-Netzwerk**

  Ermöglicht den ein-und ausgehenden Zugriff auf Intranet-Netzwerke, die der Benutzer als Home-oder work-Netzwerk festgelegt hat, oder wenn das Netzwerk einen authentifizierten Domänencontroller besitzt.

- **Internet (Client)**

  Bietet ausgehenden Zugriff auf das Internet und nicht vertrauenswürdige Netzwerke wie Flughäfen und Cafés (beispielsweise Intranet-Netzwerke, in denen der Benutzer das Netzwerk als öffentlich gekennzeichnet hat). Diese Funktion sollte von den meisten Apps verwendet werden, die einen Internetzugriff benötigen.

- **Internet (Client und Server)**

  Ermöglicht den ein-und ausgehenden Zugriff auf das Internet und nicht vertrauenswürdige Netzwerke wie Flughäfen und Cafés. Diese Funktion ist eine Obermenge der **Internet (Client)** -Funktion, und **Internet (Client)** muss nicht aktiviert werden, wenn diese Funktion aktiviert ist.

- **Näherung**

  Bietet Near-Field Communication (NFC) mit Geräten, die sich in unmittelbarer Nähe des Geräts befinden. Proximity kann verwendet werden, um Dateien zu senden oder mit einer Anwendung auf einem benachbarten Gerät zu verbinden.

Inhalt dieses Themas

Wenn Sie Microsoft Store-Apps in Ihrem Netzwerk isolieren möchten, müssen Sie die Netzwerk Isolationseinstellungen mithilfe von Gruppenrichtlinien definieren und benutzerdefinierte Firewallregeln für die Microsoft Store-App erstellen.

Voraussetzungen

- Ein Domänencontroller ist in Ihrem Netzwerk installiert, und Ihre Geräte sind mit der Windows-Domäne verbunden.
- Ihre Microsoft Store-App ist auf dem Clientgerät installiert.
- Die Remote Server-Verwaltungs Tools sind auf Ihrem Clientgerät installiert. Wenn Sie die folgenden Schritte auf Ihrem Clientgerät ausführen, können Sie die Microsoft Store-App auswählen, wenn Sie Windows Defender-Firewallregeln erstellen.

  > **Hinweis:** Sie können die Remote-Remote-Telefonzentralen auf Ihrem Gerät, auf dem Windows 10 ausgeführt wird, im Microsoft Download Centerinstallieren.

Schritt 1: Definieren Ihres Netzwerks

Die **Home\Work-Netzwerk** Funktion ermöglicht den Zugriff auf Intranet-Ressourcen. Administratoren können Gruppenrichtlinieneinstellungen verwenden, um den Bereich des Intranets zu definieren. Dadurch wird sichergestellt, dass Microsoft Store-Apps auf Intranet-Ressourcen angemessen zugreifen können.

Ein Netzwerkendpunkt wird als Teil des **Home\Work-Netzwerks** angesehen, wenn:

- Sie ist Teil des lokalen Subnetzes eines vertrauenswürdigen Netzwerks.

  So kennzeichnen private Benutzer in der Regel Ihr Netzwerk als vertrauenswürdig. Lokale Geräte werden als solche gekennzeichnet.

- Ein Gerät befindet sich in einem Netzwerk und wird von einem Domänencontroller authentifiziert.
  - Endpunkte im Intranet-Adressraum gelten als privat.
  - Endpunkte im lokalen Subnetz gelten als privat.
- Das Gerät ist für DirectAccess konfiguriert, und der Endpunkt ist Teil des Intranet-Adressraums.

Der Intranet-Adressraum umfasst konfigurierte Active Directory-Standorte und-Subnetze und ist speziell mithilfe von Gruppenrichtlinien für die Windows-Netzwerkisolierung konfiguriert. Sie können die Verwendung von Active Directory-Websites und-Subnetzen mithilfe von Gruppenrichtlinien deaktivieren, indem Sie deklarieren, dass Ihre Subnet-Definitionen autorisierend sind.

Alle Proxys, die Sie konfigurieren oder die automatisch mit Proxy-Auto Konfiguration (mithilfe des Web Proxy Auto-Discovery (WPAD)-Protokolls) konfiguriert werden, sind von der Intranetzone ausgenommen. Sie können mithilfe von Gruppenrichtlinien Proxyadressen hinzufügen.

Alle anderen Endpunkte, die die zuvor angegebenen Kriterien nicht erfüllen, gelten als Endpunkte im Internet.

So konfigurieren Sie ein GPO, das Ihren Intranet-Adressraum definiert

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungs-Snap-in (GPMC. msc), klicken Sie mit der rechten Maustaste auf die Gruppenrichtlinie, die Sie verwenden möchten, um den Adressraum zu definieren, und wählen Sie **Bearbeiten**aus.
2. Erweitern Sie im Gruppenrichtlinien-Verwaltungs-Editor **Computer Konfiguration**, erweitern Sie **Richtlinien**, erweitern Sie **Administrative Vorlagen**, erweitern Sie **Netzwerk**, und klicken Sie auf **Netzwerk Isolation**.
3. Doppelklicken Sie im rechten Bereich auf **private Netzwerkbereiche für apps**.
4. Klicken Sie im Dialogfeld **private Netzwerkbereiche für apps** auf **aktiviert**. Geben Sie im Textfeld **private** Subnetze die privaten Subnetze für Ihr Intranet ein, die bei Bedarf durch Kommas getrennt sind.

   Wenn das Contoso-Intranet beispielsweise als 10.0.0.0 mit einer Subnetzmaske von 255.255.255.0 definiert ist, geben Sie im Textfeld **private** Subnetze 10.0.0.0/24 ein.
5. Doppelklicken Sie auf **Subnet-Definitionen sind autorisierend**.

   Wenn Sie möchten, dass die zuvor erstellten Subnet-Definitionen die einzige Quelle für Ihre Subnet-Definition sind, klicken Sie auf **aktiviert**. Belassen Sie andernfalls die **nicht konfigurierte** Standardeinstellung, damit Sie zusätzliche Subnetze hinzufügen können, indem Sie lokale Einstellungen oder heuristische Netzwerkisolation verwenden.

So konfigurieren Sie die Proxyadressen für das Intranet und das Internet

1. Doppelklicken Sie auf **Internet Proxy Server für apps**. Klicken Sie auf **aktiviert**, und geben Sie dann im Textfeld **Domänen Proxys** die IP-Adressen Ihrer Internet Proxy Server ein, die durch Semikolons getrennt sind.
2. Doppelklicken Sie auf **Intranet-Proxy Server für apps**. Klicken Sie auf **aktiviert**, und geben Sie dann im Textfeld IP-Adresse die IP-Adressen Ihrer Intranet-Proxy Server ein, die durch Semikolons getrennt sind.
3. Doppelklicken Sie auf **Proxy Definitionen sind autorisierend**.

   Wenn Sie möchten, dass die von Ihnen zuvor erstellten Proxy Definitionen die einzige Quelle für Ihre Proxy Definition sind, klicken Sie auf **aktiviert**. Belassen Sie andernfalls die **nicht konfigurierte** Standardeinstellung, damit Sie zusätzliche Proxys hinzufügen können, indem Sie lokale Einstellungen oder heuristische Netzwerkisolation verwenden.

Schritt 2: Erstellen benutzerdefinierter Firewallregeln

Microsoft Store-Apps können zusätzlich zu den zuvor besprochenen Netzwerkfunktionen viele Funktionen deklarieren. Beispielsweise können apps Funktionen für den Zugriff auf die Benutzeridentität, das lokale Dateisystem und bestimmte Hardwaregeräte deklarieren.

Die folgende Tabelle enthält eine vollständige Liste der möglichen App-Funktionen.

FUNKTION	NAME	BESCHREIBUNG
Internet (Client)	internetClient	Ihre ausgehende Internet Verbindung.

FUNKTION	NAME	BESCHREIBUNG
Internet (Client & Server)	internetClientServer	Ihre Internetverbindung, einschließlich eingehender unerwünschter Verbindungen aus dem Internet die APP kann über eine Firewall Informationen an oder von Ihrem Gerät senden. Sie müssen **Internet Client** nicht deklarieren, wenn diese Funktion deklariert wurde.
Home\Work-Netzwerk	privateNetworkClientServer	Ein Home-oder work-Netzwerk. Die APP kann Informationen an oder von Ihrem Gerät und anderen Geräten im gleichen Netzwerk senden.
Zugriff auf Dokumentbibliothek	documentsLibrary	Ihre Dokumentbibliothek, einschließlich der Möglichkeit, Dateien hinzuzufügen, zu ändern oder zu löschen. Das Paket kann nur auf Dateitypen zugreifen, die im Manifest deklariert sind.
Zugriff auf Bildbibliothek	picturesLibrary	Ihre Bildbibliothek, einschließlich der Möglichkeit, Dateien hinzuzufügen, zu ändern oder zu löschen.
Zugriff auf Video Bibliothek	videosLibrary	Ihre Videobibliothek, einschließlich der Möglichkeit, Dateien hinzuzufügen, zu ändern oder zu löschen.
Zugriff auf Musikbibliothek	musicLibrary	Ihre Musikbibliothek, einschließlich der Möglichkeit, Dateien hinzuzufügen, zu ändern oder zu löschen.
Standardmäßige Windows-Anmeldeinformationen	defaultWindowsCredentials	Ihre Windows-Anmeldeinformationen für den Zugriff auf ein Unternehmensintranet. Diese Anwendung kann Sie im Netzwerk anweisen.
Wechselmedien	removableStorage	Ein Wechselspeichergerät wie eine externe Festplatte, ein USB-Flashlaufwerk oder ein tragbares MTP-Gerät, einschließlich der Möglichkeit, bestimmte Dateien hinzuzufügen, zu ändern oder zu löschen. Dieses Paket kann nur auf Dateitypen zugreifen, die im Manifest deklariert sind.
Freigegebene Benutzerzertifikate	sharedUserCertificates	Software-und Hardware Zertifikate oder eine Smartcard, die von der APP verwendet wird, um Sie zu identifizieren. Diese Funktion kann von einem Arbeitgeber, einer Bank oder staatlichen Dienstleistungen genutzt werden, um Sie zu identifizieren.
Standort	Lage	Bietet Zugriff auf den aktuellen Standort des Benutzers.

FUNKTION	NAME	BESCHREIBUNG
Mikrofon	Mikrofon	Bietet Zugriff auf den Audiofeed des Mikrofons.
Near-Field-Näherung	proximity	Erforderlich für nahfeldkommunikation (NFC) zwischen Geräten in unmittelbarer Nähe. NFC kann zum Senden von Dateien oder zum Herstellen einer Verbindung mit einer APP auf einem unmittelbaren Gerät verwendet werden.
Text Nachrichten	SMS	Bietet Zugriff auf Funktionen für Textnachrichten.
Webcam	Webcam	Bietet Zugriff auf den Video-Feed der Webcam.
Andere Geräte (durch GUIDs dargestellt)	<GUID>	Umfasst spezielle Geräte und tragbare Windows-Geräte.

Sie können eine Windows Defender-Firewall-Richtlinie erstellen, die sich auf eine Reihe von apps beläuft, die eine bestimmte Funktion verwenden oder auf eine bestimmte Microsoft Store-App beschränkt sind.

So können Sie beispielsweise eine Windows Defender-Firewall-Richtlinie erstellen, um den Internet Zugriff für alle apps in Ihrem Netzwerk zu blockieren, die über die Bibliotheksfunktion "Dokumente" verfügen.

So blockieren Sie den Internet Zugriff für alle apps in Ihrem Netzwerk, die über die Bibliotheksfunktion "Dokumente" verfügen

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungs-Snap-in (GPMC. msc).
2. Klicken Sie im linken Bereich mit der rechten Maustaste auf Ihren Domänennamen, und klicken Sie dann auf **Gruppenrichtlinienobjekt in dieser Domäne erstellen, und verknüpfen Sie es hier**.
3. Geben Sie im Textfeld **Name** einen Namen für das Gruppenrichtlinienobjekt ein, und klicken Sie dann auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf das neue Gruppenrichtlinienobjekt, und klicken Sie dann auf **Bearbeiten**.
5. Erweitern Sie im Gruppenrichtlinien-Verwaltungs-Editor **Computer Konfiguration**, erweitern Sie **Richtlinien**, erweitern Sie **Windows-Einstellungen**, erweitern Sie **Sicherheitseinstellungen**, erweitern Sie **Windows Defender Firewall mit erweiterter Sicherheit**, und klicken Sie auf **Windows Defender-Firewall – LDAP://...**
6. Klicken Sie mit der rechten Maustaste auf **Ausgehende Regeln**, und klicken Sie dann auf **Neue Regel**.
7. Klicken Sie auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.
8. Klicken Sie auf der Seite **Programm** , auf der Seite **Protokolle und Ports** und auf der Seite **Bereich** auf **weiter** .
9. Stellen Sie auf der Seite **Aktion** sicher, dass **die Verbindung blockieren** ausgewählt ist, und klicken Sie dann auf **weiter**.
10. Klicken Sie auf der Seite **Profil** auf **weiter**.
11. Geben Sie auf der Seite **Name** einen Namen für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

12. Klicken Sie im rechten Bereich mit der rechten Maustaste auf die neue Regel, und klicken Sie auf **Eigenschaften**.
13. Klicken Sie auf die Registerkarte **lokale Prinzipale** , aktivieren Sie das Kontrollkästchen **nur Verbindungen von diesen Benutzern zulassen** , und klicken Sie dann auf **Hinzufügen**.
14. Klicken Sie auf **Anwendungspaket Eigenschaften**, und klicken Sie dann auf **OK**.
15. Klicken Sie im Dialogfeld **Funktionen auswählen** auf **Anwendungspaket-AUTHORITY\Your-Dokumentbibliothek**, und klicken Sie dann auf **OK**.
16. Klicken Sie auf die Registerkarte **Bereich** unter **Remote-IP-Adressen**, und klicken Sie dann auf **Hinzufügen**.
17. Klicken Sie auf vordefinierte **Gruppe von Computern**, wählen Sie **Internet**aus, und klicken Sie auf **OK**.

    Dadurch wird die Regel zum Blockieren des Datenverkehrs zu Internet Geräten Bereich.
18. Klicken Sie auf die Registerkarte **Programme und Dienste** , und klicken Sie im Bereich **Anwendungspakete** auf **Einstellungen**.
19. Klicken Sie auf **nur Anwendungspakete übernehmen**, und klicken Sie dann auf **OK**.

    > **Wichtig:** Sie müssen dies tun, um sicherzustellen, dass die Regel nur für Microsoft Store-Apps und nicht für andere apps gilt. Desktop-Apps deklarieren standardmäßig alle Funktionen, und diese Regel würde auf Sie zutreffen, wenn Sie Sie nicht auf diese Weise konfigurieren.
20. Klicken Sie auf **OK** , um das Dialogfeld **Eigenschaften** zu schließen.
21. Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.
22. Stellen Sie im Gruppenrichtlinien Verwaltungs-Snap-in sicher, dass Ihr neues Gruppenrichtlinienobjekt ausgewählt ist, und wählen Sie im rechten Bereich unter **Sicherheitsfilterung**die Option **Authentifizierte Benutzer**aus. Klicken Sie auf **Entfernen**, und klicken Sie dann auf **OK**.
23. Klicken Sie unter **Sicherheitsfilterung**auf **Hinzufügen**.
24. Geben Sie im Textfeld **Domänencomputer** ein, und klicken Sie dann auf **OK**.
25. Schließen Sie das Gruppenrichtlinien-Verwaltungs-Snap-in.

Führen Sie die folgenden Schritte aus, wenn Sie den Intranet-Zugriff für eine bestimmte Medienfreigabe-app in Ihrem Netzwerk blockieren möchten.

So blockieren Sie den Intranet-Zugriff für eine bestimmte Medienfreigabe-app in Ihrem Netzwerk

1. Öffnen Sie das Gruppenrichtlinien-Verwaltungs-Snap-in (GPMC. msc).
2. Klicken Sie im linken Bereich mit der rechten Maustaste auf Ihren Domänennamen, und klicken Sie dann auf **Gruppenrichtlinienobjekt in dieser Domäne erstellen, und verknüpfen Sie es hier**.
3. Geben Sie im Textfeld **Name** einen Namen für das Gruppenrichtlinienobjekt ein, und klicken Sie dann auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf das neue GPO, und klicken Sie dann auf **Bearbeiten**.
5. Erweitern Sie im Gruppenrichtlinien-Verwaltungs-Editor **Computer Konfiguration**, erweitern Sie **Richtlinien**, erweitern Sie **Windows-Einstellungen**, erweitern Sie **Sicherheitseinstellungen**, erweitern Sie **Windows Defender Firewall**, und klicken Sie dann auf **Windows. Defender Firewall – LDAP://**...
6. Klicken Sie mit der rechten Maustaste auf **Ausgehende Regeln**, und klicken Sie dann auf **Neue Regel**.

7. Klicken Sie auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.
8. Klicken Sie auf der Seite **Programm** , auf der Seite **Protokolle und Ports** und auf der Seite **Bereich** auf **weiter** .
9. Stellen Sie auf der Seite **Aktion** sicher, dass **die Verbindung blockieren** ausgewählt ist, und klicken Sie dann auf **weiter**.
10. Klicken Sie auf der Seite **Profil** auf **weiter**.
11. Geben Sie auf der Seite **Name** einen Namen für die Regel ein, und klicken Sie dann auf **Fertig stellen**.
12. Klicken Sie im rechten Bereich mit der rechten Maustaste auf die neue Regel, und klicken Sie dann auf **Eigenschaften**.
13. Klicken Sie auf die Registerkarte **lokale Prinzipale** , aktivieren Sie das Kontrollkästchen **nur Verbindungen von diesen Benutzern zulassen** , und klicken Sie dann auf **Hinzufügen**.
14. Klicken Sie auf **Anwendungspaket Eigenschaften**, und klicken Sie dann auf **OK**.
15. Klicken Sie im Dialogfeld **Funktionen auswählen** auf **Anwendungspaket AUTHORITY\A Home oder Work Network**, und klicken Sie dann auf **OK**.
16. Klicken Sie unter **Anwendungspakete**auf die Registerkarte **Programme und Dienste** , und klicken Sie dann auf **Einstellungen**.
17. Klicken Sie auf **für dieses Anwendungspaket übernehmen**, wählen Sie die APP im Textfeld aus, und klicken Sie dann auf **OK**.
18. Klicken Sie auf **OK** , um das Dialogfeld **Eigenschaften** zu schließen.
19. Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.
20. Stellen Sie in der Gruppenrichtlinienverwaltung sicher, dass Ihr neues Gruppenrichtlinienobjekt ausgewählt ist, und wählen Sie im rechten Bereich unter **Sicherheitsfilterung Authentifizierte Benutzer**aus, klicken Sie auf **Entfernen**, und klicken Sie dann auf **OK**.
21. Klicken Sie unter **Sicherheitsfilterung**auf **Hinzufügen**.
22. Geben Sie im Textfeld **Domänencomputer** ein, und klicken Sie auf **OK**.
23. Schließen Sie die Gruppenrichtlinienverwaltung.

Weitere Informationen:

- Windows Defender-Firewall mit erweiterter Sicherheitsübersicht

Sichern von End-to-End-IPSec-Verbindungen mithilfe von IKEv2

10.06.2019 • 5 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

IKEv2 bietet Folgendes an:

- Unterstützt Verbindungen zwischen IPSec-End-to-End-Transportmodus
- Bietet Interoperabilität für Windows mit anderen Betriebssystemen, die IKEv2 für die End-to-End-Sicherheit verwenden
- Unterstützt Anforderungen für Suite B (RFC 4869)
- Koexistiert mit vorhandenen Richtlinien, die AuthIP/ikev1 bereitstellen
- Verwendet die Windows PowerShell-Schnittstelle exklusiv für die Konfiguration. Sie können IKEv2 nicht über die Benutzeroberfläche konfigurieren.
- Verwendet Zertifikate für den Authentifizierungsmechanismus

Sie können IKEv2 als VPN-Tunneling-Protokoll (virtuelles privates Netzwerk) verwenden, das die automatische VPN-erneute Verbindung unterstützt. IKEv2 ermöglicht es, dass die Sicherheitszuordnung trotz Änderungen in der zugrunde liegenden Verbindung unverändert bleibt.

In diesem Dokument

> **Hinweis:** dieses Thema enthält Beispiel-Windows PowerShell-Cmdlets. Weitere Informationen finden Sie unter so wird es gemacht: Ausführen eines Windows PowerShell-Cmdlets.

Voraussetzungen

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits über eine Public Key-Infrastruktur (PKI) für die Geräteauthentifizierung verfügen.

Geräte, die einer Domäne beigetreten sind

Das folgende Windows PowerShell-Skript richtet eine Verbindungssicherheitsregel ein, die IKEv2 für die Kommunikation zwischen zwei Computern (CLIENT1 und Server1) verwendet, die mit der Corp.contoso.com-Domäne verbunden sind, wie in Abbildung1 dargestellt.

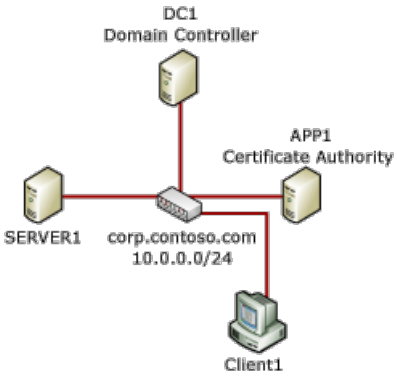


Abbildung1 Das Unternehmensnetzwerk von Contoso

Dieses Skript führt die folgenden Aktionen aus:

- Erstellt eine Sicherheitsgruppe namens **IPSec-Client und-Server** und fügt CLIENT1 und server1 als Mitglieder hinzu.
- Erstellt ein Gruppenrichtlinienobjekt mit dem Namen **IPsecRequireInRequestOut** und verknüpft es mit der Corp.contoso.com-Domäne.
- Legt die Berechtigungen für das Gruppenrichtlinienobjekt so fest, dass Sie nur für die Computer in **IPSec-Client und-Server** und nicht für **Authentifizierte Benutzer**gelten.
- Gibt das Zertifikat an, das für die Authentifizierung verwendet werden soll.

  > **Wichtig:** bei den für das Zertifikat angegebenen Zertifikat Parametern muss die Groß-/Kleinschreibung beachtet werden, stellen Sie daher sicher, dass Sie diese genau wie im Zertifikat angegeben eingeben, und fügen Sie die Parameter in der exakten Reihenfolge ein, die Sie im folgenden Beispiel sehen. Wenn dies nicht der Fall ist, entstehen Verbindungsfehler.

- Erstellt die IKEv2-Verbindungssicherheitsregel, die als **meine IKEv2-Regel**bezeichnet wird.

Windows PowerShell-Befehle

Geben Sie die einzelnen Cmdlets in einer einzelnen Zeile ein, auch wenn Sie aufgrund von Formatierungseinschränkungen möglicherweise über mehrere Zeilen umbrochen werden.

```
# Create a Security Group for the computers that will get the policy
$pathname = (Get-ADDomain).distinguishedname
New-ADGroup -name "IPsec client and servers" -SamAccountName "IPsec client and servers" `
-GroupCategory security -GroupScope Global -path $pathname

# Add test computers to the Security Group
$computer = Get-ADComputer -LDAPFilter "(name=client1)"
Add-ADGroupMember -Identity "IPsec client and servers" -Members $computer
$computer = Get-ADComputer -LDAPFilter "(name=server1)"
Add-ADGroupMember -Identity "IPsec client and servers" -Members $computer

# Create and link the GPO to the domain
$gpo = New-gpo IPsecRequireInRequestOut
$gpo | new-gplink -target "dc=corp,dc=contoso,dc=com" -LinkEnabled Yes

# Set permissions to security group for the GPO
$gpo | Set-GPPermissions -TargetName "IPsec client and servers" -TargetType Group -PermissionLevel GpoApply -
Replace
$gpo | Set-GPPermissions -TargetName "Authenticated Users" -TargetType Group -PermissionLevel None -Replace

#Set up the certificate for authentication
$gponame = "corp.contoso.com\IPsecRequireInRequestOut"
$certprop = New-NetIPsecAuthProposal -machine -cert -Authority "DC=com, DC=contoso, DC=corp, CN=corp-APP1-CA"
$myauth = New-NetIPsecPhase1AuthSet -DisplayName "IKEv2TestPhase1AuthSet" -proposal $certprop –PolicyStore
GPO:$gponame

#Create the IKEv2 Connection Security rule
New-NetIPsecRule  -DisplayName "My IKEv2 Rule" -RemoteAddress any -Phase1AuthSet $myauth.InstanceID `
-InboundSecurity Require -OutboundSecurity Request -KeyModule IKEv2 -PolicyStore GPO:$gponame
```

Geräte, die nicht mit einer Domäne verbunden sind

Verwenden Sie ein Windows PowerShell-Skript, das der folgenden ähnelt, um eine lokale IPSec-Richtlinie auf den Geräten zu erstellen, die Sie in die sichere Verbindung einbeziehen möchten.

> **Wichtig:** bei den für das Zertifikat angegebenen Zertifikat Parametern muss die Groß-/Kleinschreibung beachtet werden, stellen Sie daher sicher, dass Sie diese genau wie im Zertifikat angegeben eingeben, und fügen Sie die Parameter in der exakten Reihenfolge ein, die Sie im folgenden Beispiel sehen. Wenn dies nicht der Fall ist, entstehen Verbindungsfehler.

Windows PowerShell-Befehle

Geben Sie die einzelnen Cmdlets in einer einzelnen Zeile ein, auch wenn Sie aufgrund von Formatierungseinschränkungen möglicherweise über mehrere Zeilen umbrochen werden.

```
#Set up the certificate
$certprop = New-NetIPsecAuthProposal -machine -cert -Authority "DC=com, DC=contoso, DC=corp, CN=corp-APP1-CA"
$myauth = New-NetIPsecPhase1AuthSet -DisplayName "IKEv2TestPhase1AuthSet" -proposal $certprop

#Create the IKEv2 Connection Security rule
New-NetIPsecRule  -DisplayName "My IKEv2 Rule" -RemoteAddress any -Phase1AuthSet $myauth.InstanceID `
-InboundSecurity Require -OutboundSecurity Request -KeyModule IKEv2
```

Stellen Sie sicher, dass Sie die erforderlichen Zertifikate auf den teilnehmenden Computern installieren.

> **Hinweis:**
>
> - Bei lokalen Geräten können Sie die Zertifikate manuell importieren, wenn Sie über Administratorzugriff auf den Computer verfügen. Weitere Informationen finden Sie unter importieren oder Exportieren von

Zertifikaten und privaten Schlüsseln.

- Sie benötigen ein Stammzertifikat und ein Computerzertifikat auf allen Geräten, die an der sicheren Verbindung teilnehmen. Speichern Sie das Computerzertifikat im Ordner " **Personal/Zertifikate** ".
- Bei Remotegeräten können Sie eine sichere Website erstellen, um den Zugriff auf das Skript und die Zertifikate zu erleichtern.

Problembehandlung

Führen Sie die folgenden Verfahren aus, um Ihre IPSec-IKEv2-Verbindungen zu überprüfen und zu beheben:

Verwenden Sie das Snap-in Windows Defender-Firewall mit erweiterter Sicherheit, um zu überprüfen, ob eine Verbindungssicherheitsregel aktiviert ist.

1. Öffnen Sie die Windows Defender-Firewall mit erweiterter Sicherheitskonsole.
2. Klicken Sie im linken Bereich des Snap-Ins Windows Defender-Firewall mit erweiterter Sicherheit auf **Verbindungssicherheitsregeln**, und überprüfen Sie dann, ob eine Verbindungssicherheitsregel aktiviert ist.
3. Erweitern Sie **Überwachung**, und klicken Sie dann auf **Verbindungssicherheitsregeln** , um zu überprüfen, ob Ihre IKEv2-Regel für Ihr aktuell aktives Profil aktiv ist.

Verwenden Sie Windows PowerShell-Cmdlets, um die Sicherheitszuordnungen anzuzeigen.

1. Öffnen Sie eine Windows PowerShell-Eingabeaufforderung.
2. Geben **Sie Get-NetIPsecQuickModeSA** ein, um die Schnellmodus-Sicherheitszuordnungen anzuzeigen.
3. Geben **Sie Get-NetIPsecMainModeSA** ein, um die Hauptmodus-Sicherheitszuordnungen anzuzeigen.

Verwenden Sie netsh zum Aufzeichnen von IPSec-Ereignissen.

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie an der Eingabeaufforderung **netsh wfp capture Start**ein.
3. Reproduzieren Sie das Fehlerereignis, damit es erfasst werden kann.
4. Geben Sie an der Eingabeaufforderung **netsh wfp capture stop**ein.

   Eine wfpdiag. CAB-Datei wird im aktuellen Ordner erstellt.
5. Öffnen Sie die CAB-Datei, und extrahieren Sie die Datei "wfpdiag. xml".
6. Öffnen Sie die Datei "wfpdiag. xml" mit einem XML-Viewer-Programm oder-Editor, und überprüfen Sie dann den Inhalt. Diese Datei enthält viele Daten. Eine Möglichkeit zur Eingrenzung des Ausgangspunkts besteht darin, das letzte "errorFrequencyTable" am Ende der Datei zu durchsuchen. Es können viele Instanzen dieser Tabelle vorhanden sein, stellen Sie daher sicher, dass Sie die letzte Tabelle in der Datei sehen. Wenn Sie beispielsweise ein Zertifikatproblem haben, wird möglicherweise der folgende Eintrag in der letzten Tabelle am Ende der Datei angezeigt:

   ```
   <item>
     <error>ERROR_IPSEC_IKE_NO_CERT</error>
     <frequency>32</frequency>
   </item>
   ```

   In diesem Beispiel gibt es 32-Instanzen des **ERROR_IPSEC_IKE_NO_CERT** -Fehlers. Nun können Sie nach **ERROR_IPSEC_IKE_NO_CERT** suchen, um weitere Informationen zu diesem Fehler zu erhalten.

Möglicherweise finden Sie die genaue Antwort für das Problem nicht, aber Sie können gute Hinweise finden. So können Sie beispielsweise feststellen, dass ein Problem mit den Zertifikaten vorliegt, sodass Sie Ihre Zertifikate und die zugehörigen Cmdlets auf mögliche Probleme hinweisen können.

Weitere Informationen:

- Windows Defender-Firewall mit erweiterter Sicherheit

Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell

01.06.2019 • 22 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell-Handbuch bietet grundlegende Scriptlets für die Automatisierung der Windows Defender-Firewallverwaltung. Sie ist für IT-Experten, Systemadministratoren, IT-Manager und andere Personen konzipiert, die die Windows Defender-Firewallverwaltung in Windows verwenden und automatisieren müssen.

Sie können Windows PowerShell verwenden, um Ihre Firewall-und IPsec-Bereitstellungen zu verwalten. Mit dieser objektorientierten Skriptumgebung können Sie Richtlinien einfacher verwalten und Netzwerkbedingungen überwachen, als dies in netsh möglich war. Mit Windows PowerShell können Netzwerkeinstellungen über die Syntax und die Parameter in den einzelnen Cmdlets selbst erkannt werden. Dieser Leitfaden zeigt, wie allgemeine Aufgaben in netsh ausgeführt wurden und wie Sie Sie mithilfe von Windows PowerShell ausführen können.

In zukünftigen Versionen von Windows kann Microsoft die Netsh-Funktionalität für Windows Defender Firewall entfernen. Microsoft empfiehlt, dass Sie zu Windows PowerShell wechseln, wenn Sie derzeit netsh zum Konfigurieren und Verwalten der Windows Defender-Firewall verwenden.

Windows PowerShell-und Netsh-Befehls Verweise befinden sich an den folgenden Speicherorten.

- Netsh-Befehle für Windows Defender-Firewall

Bereich

Dieses Handbuch vermittelt Ihnen nicht die Grundlagen der Windows Defender-Firewall, die in der Windows Defender-Firewallzu finden sind. Es werden nicht die Grundlagen von Windows PowerShell vermittelt, und es wird davon ausgegangen, dass Sie mit der Windows PowerShell-Sprache und den grundlegenden Konzepten von Windows PowerShell vertraut sind. Weitere Informationen zu Windows PowerShell-Konzepten und-Verwendung finden Sie in diesem Leitfaden unter den Referenzthemen im Abschnitt zusätzliche Ressourcen .

Zielgruppen-und Benutzeranforderungen

Dieses Handbuch richtet sich an IT-Experten, Systemadministratoren und IT-Manager, und es wird davon ausgegangen, dass Sie mit der Windows Defender-Firewall, der Windows PowerShell-Sprache und den grundlegenden Konzepten von Windows PowerShell vertraut sind.

Inhalt dieses Themas

ABSCHNITT	BESCHREIBUNG
Festlegen globaler Standardwerte für profile	Aktivieren und Steuern des Firewall-Verhaltens
Bereitstellen von grundlegenden Firewallregeln	Erstellen, ändern und Löschen von Firewallregeln

ABSCHNITT	BESCHREIBUNG
Remoteverwaltung	Remote Verwaltung mithilfe von `-CimSession`
Bereitstellen von grundlegenden IPSec-Regeleinstellungen	IPSec-Regeln und zugeordnete Parameter
Bereitstellen von sicheren Firewallregeln mit IPSec	Domänen-und Serverisolierung
Zusätzliche Ressourcen	Weitere Informationen zu Windows PowerShell

Festlegen globaler Standardwerte für profile

Mit globalen Standardeinstellungen wird das Geräte Verhalten in einer einzelnen Profilebene eingestellt. Die Windows Defender-Firewall unterstützt Domänen-, private und öffentliche Profile.

Aktivieren der Windows Defender-Firewall mit erweiterter Sicherheit

Die Windows Defender-Firewall löscht Datenverkehr, der nicht dem zulässigen nicht angeforderten Datenverkehr entspricht, oder Datenverkehr, der als Antwort auf eine Anforderung des Geräts gesendet wird. Wenn Sie feststellen, dass die von Ihnen erstellten Regeln nicht erzwungen werden, müssen Sie möglicherweise die Windows Defender-Firewall aktivieren. Hier erfahren Sie, wie Sie dies auf einem lokalen Domänen Gerät ausführen:

Netsh

```
netsh advfirewall set allprofiles state on
```

Windows PowerShell

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
```

Steuern der Windows Defender-Firewall mit erweitertem Sicherheitsverhalten

Die globalen Standardeinstellungen können über die Befehlszeilenschnittstelle definiert werden. Diese Änderungen stehen auch über die Windows Defender-Firewall mit erweiterter Sicherheitskonsole zur Verfügung.

Die folgenden Scriptlets Festlegen der standardmäßigen ein-und ausgehenden Aktionen, gibt geschützte Netzwerkverbindungen an und ermöglicht dem Benutzer die Anzeige von Benachrichtigungen, wenn ein Programm vom empfangen von eingehenden Verbindungen blockiert wird. Sie ermöglicht Unicast-Antwort auf Multicast-oder Broadcast-Netzwerkdatenverkehr und gibt Protokollierungseinstellungen für die Problembehandlung an.

Netsh

```
netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound
netsh advfirewall set allprofiles settings inboundusernotification enable
netsh advfirewall set allprofiles settings unicastresponsetomulticast enable
netsh advfirewall set allprofiles logging filename %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log
```

Windows PowerShell

```
Set-NetFirewallProfile -DefaultInboundAction Block -DefaultOutboundAction Allow –NotifyOnListen True -
AllowUnicastResponseToMulticast True –LogFileName %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log
```

Deaktivieren der Windows Defender-Firewall mit erweiterter Sicherheit

Microsoft empfiehlt, die Windows Defender-Firewall nicht zu deaktivieren, da andere vom Dienst bereitgestellte Vorteile verloren gehen, beispielsweise die Möglichkeit, IPsec-Verbindungssicherheitsregeln (Internet Protocol Security) zu verwenden, Netzwerkschutz vor Angriffen, die Netzwerk-Fingerabdruck, Windows-Diensthärtungund Startzeitfilter.

Das Deaktivieren der Windows Defender-Firewall mit erweiterter Sicherheit kann auch zu Problemen führen, einschließlich:

- Das Startmenü kann nicht mehr funktionieren
- Moderne Anwendungen können nicht installiert oder aktualisiert werden
- Die Aktivierung von Windows über das Telefon schlägt fehl
- Anwendungs-oder Betriebssystem Inkompatibilitäten, die von der Windows Defender-Firewall abhängen

Microsoft empfiehlt, die Windows Defender-Firewall nur bei der Installation einer Drittanbieter-Firewall zu deaktivieren und die Windows Defender-Firewall wieder auf Standardwerte zurückzusetzen, wenn die Software eines Drittanbieters deaktiviert oder entfernt wird.

Wenn die Deaktivierung der Windows Defender-Firewall erforderlich ist, deaktivieren Sie Sie nicht, indem Sie den Windows Defender-Firewalldienst beenden (im **Dienste** -Snap-in ist der Anzeigename Windows Defender Firewall und der Dienstname MpsSvc). Das Beenden des Windows Defender-Firewall-Diensts wird von Microsoft nicht unterstützt.

Eine nicht von Microsoft Firewall-Software kann programmgesteuert nur die Teile der Windows Defender-Firewall deaktivieren, die aus Kompatibilitätsgründen deaktiviert werden müssen. Sie sollten die Firewall für diesen Zweck nicht selbst deaktivieren.

Die richtige Methode zum Deaktivieren der Windows Defender-Firewall besteht darin, die Windows Defender-Firewall-Profile zu deaktivieren und den Dienst ausgeführt zu lassen.

Gehen Sie wie folgt vor, um die Firewall zu deaktivieren, oder deaktivieren Sie die Gruppenrichtlinieneinstellung **Computer Konfiguration | Administrative Vorlagen | Netzwerk | Netzwerkverbindungen | Windows Defender-Firewall | Domäne proldatei | Windows Defender-Firewall: schützen Sie alle Netzwerkverbindungen**. Weitere Informationen finden Sie unter Windows Defender Firewall with Advanced Security Deployment Guide.

Im folgenden Beispiel wird die Windows Defender-Firewall für alle Profile deaktiviert.

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

Bereitstellen von grundlegenden Firewallregeln

Dieser Abschnitt enthält Scriptlet-Beispiele für das Erstellen, ändern und Löschen von Firewall-Regeln.

Erstellen von Firewallregeln

Das Hinzufügen einer Firewallregel in Windows PowerShell ähnelt viel wie in netsh, aber die Parameter und Werte werden anders angegeben.

Im folgenden finden Sie ein Beispiel dafür, wie die Telnet-Anwendung das Netzwerk überwachen kann. Diese Firewallregel wird mit einem Schlüsselwort anstelle einer IP-Adresse auf das lokale Subnetz begrenzt. Genau wie in netsh wird die Regel auf dem lokalen Gerät erstellt und sofort wirksam.

Netsh

```
netsh advfirewall firewall add rule name="Allow Inbound Telnet" dir=in program=
%SystemRoot%\System32\tlntsvr.exe remoteip=localsubnet action=allow
```

Windows PowerShell

```
New-NetFirewallRule -DisplayName “Allow Inbound Telnet” -Direction Inbound -Program
%SystemRoot%\System32\tlntsvr.exe -RemoteAddress LocalSubnet -Action Allow
```

Die folgende Scriptlet zeigt, wie Sie eine grundlegende Firewall-Regel hinzufügen, die ausgehenden Datenverkehr von einer bestimmten Anwendung und einem lokalen Port zu einem Gruppenrichtlinienobjekt (GPO) in Active Directory blockiert. In Windows PowerShell wird der Richtlinienspeicher als Parameter innerhalb des Cmdlets **New-netfirewall** angegeben. In netsh müssen Sie zuerst das Gruppenrichtlinienobjekt angeben, das von den Befehlen in einer Netsh-Sitzung geändert werden soll. Die von Ihnen eingegebenen Befehle werden für den Inhalt des Gruppenrichtlinienobjekts ausgeführt, und dieser bleibt in Kraft, bis die Netsh-Sitzung beendet wird oder ein weiterer Befehl für den Satz Speicher ausgeführt wird.

Hier ist **Domain.contoso.com** der Name Ihrer Active Directory-Domänendienste (Adds), und **gpo_name** ist der Name des Gruppenrichtlinienobjekts, das Sie ändern möchten. Anführungszeichen sind erforderlich, wenn der GPO-Name Leerzeichen enthält.

Netsh

```
netsh advfirewall set store gpo=domain.contoso.com\gpo_name
netsh advfirewall firewall add rule name="Block Outbound Telnet" dir=out
program=%SystemRoot%\System32\telnet.exe protocol=tcp localport=23 action=block
```

Windows PowerShell

```
New-NetFirewallRule -DisplayName “Block Outbound Telnet” -Direction Outbound -Program
%SystemRoot%\System32\tlntsvr.exe –Protocol TCP –LocalPort 23 -Action Block –PolicyStore
domain.contoso.com\gpo_name
```

Zwischenspeicherung von Gruppenrichtlinienobjekten

Um die Belastung für Beschäftigte Domänencontroller zu verringern, können Sie mithilfe von Windows PowerShell ein GPO in Ihre lokale Sitzung laden, alle Ihre Änderungen in dieser Sitzung vornehmen und es dann einmal wieder speichern.

Im folgenden werden die gleichen Aktionen wie im vorherigen Beispiel durchgeführt (durch Hinzufügen einer Telnet-Regel zu einem Gruppenrichtlinienobjekt), dies ist jedoch die Nutzung der GPO-Zwischenspeicherung in PowerShell. Das Ändern des Gruppenrichtlinienobjekts durch das Laden in Ihre lokale Sitzung und die Verwendung des *-GPOSession-* Parameters werden in netsh nicht unterstützt.

Windows PowerShell

```
$gpo = Open-NetGPO –PolicyStore domain.contoso.com\gpo_name
New-NetFirewallRule -DisplayName “Block Outbound Telnet” -Direction Outbound -Program
%SystemRoot%\System32\telnet.exe –Protocol TCP –LocalPort 23 -Action Block –GPOSession $gpo
Save-NetGPO –GPOSession $gpo
```

Beachten Sie, dass dadurch die einzelnen Änderungen nicht in den Stapel fallen, sondern das gesamte Gruppenrichtlinienobjekt gleichzeitig geladen und gespeichert werden. Wenn andere Administratoren oder in einem anderen Windows PowerShell-Fenster andere Änderungen vornehmen, werden diese Änderungen durch Speichern des Gruppenrichtlinienobjekts überschrieben.

Ändern einer vorhandenen Firewall-Regel

Wenn eine Regel erstellt wird, können Sie mithilfe von Netsh und Windows PowerShell Regeleigenschaften und-Einflüsse ändern, aber die Regel behält ihren eindeutigen Bezeichner bei (in Windows PowerShell wird dies mit dem *-Name-* Parameter angegeben).

Sie können beispielsweise eine Regel zulassen, dass **Web 80** , die TCP-Port 80 für eingehenden unerwünschten Datenverkehr aktiviert. Sie können die Regel so ändern, dass Sie einer anderen Remote-IP-Adresse eines Webservers entspricht, deren Datenverkehr zulässig ist, indem Sie den Benutzer lesbaren, lokalisierten Namen der Regel angeben.

Netsh

```
netsh advfirewall firewall set rule name="Allow Web 80" new remoteip=192.168.0.2
```

Windows PowerShell

```
Set-NetFirewallRule –DisplayName “Allow Web 80” -RemoteAddress 192.168.0.2
```

Für netsh müssen Sie den Namen der Regel angeben, damit Sie geändert werden kann, und wir haben keine alternative Möglichkeit, die Firewallregel zu erhalten. In Windows PowerShell können Sie die Regel mithilfe der bekannten Eigenschaften Abfragen.

Wenn Sie Ausführen `Get-NetFirewallRule`, stellen Sie möglicherweise fest, dass allgemeine Bedingungen wie Adressen und Ports nicht angezeigt werden. Diese Bedingungen werden in separaten Objekten namens "Filter" dargestellt. Wie zuvor gezeigt, können Sie alle Bedingungen in New-NetFirewallRule und NetFirewallRule. Wenn Sie auf der Grundlage dieser Felder (Ports, addresses, Security, Interfaces, Services) Firewall-Regeln Abfragen möchten, müssen Sie die Filterobjekte selbst abrufen.

Sie können den Remoteendpunkt der Regel " **Web 80 zulassen** " (wie zuvor ausgeführt) mithilfe von Filterobjekten ändern. Bei Verwendung von Windows PowerShell, die Sie mithilfe des Port Filters nach Port Abfragen, wird angenommen, dass zusätzliche Regeln vorhanden sind, die sich auf den lokalen Port auswirken, und Sie erstellen mit weiteren Abfragen, bis die gewünschte Regel abgerufen wurde.

Im folgenden Beispiel wird davon ausgegangen, dass die Abfrage eine einzelne Firewallregel zurückgibt, die dann mithilfe `Set-NetFirewallRule` der Fähigkeit von Windows PowerShell zur Pipelineeingabe an das Cmdlet weitergeleitet wird.

Windows PowerShell

```
Get-NetFirewallPortFilter | ?{$_.LocalPort -eq 80} | Get-NetFirewallRule | ?{ $_.Direction –eq “Inbound” -and
$_.Action –eq “Allow”} | Set-NetFirewallRule -RemoteAddress 192.168.0.2
```

Sie können auch mithilfe des Platzhalterzeichens Abfragen für Regeln durch stellen. Im folgenden Beispiel wird ein Array mit Firewallregeln zurückgegeben, die einem bestimmten Programm zugeordnet sind. Die Elemente des Arrays können in nachfolgenden `Set-NetFirewallRule` Cmdlets geändert werden.

Windows PowerShell

```
Get-NetFirewallApplicationFilter -Program "*svchost*" | Get-NetFirewallRule
```

Mehrere Regeln in einer Gruppe können gleichzeitig geändert werden, wenn der zugeordnete Gruppenname in einem Satz Befehl angegeben wird. Sie können bestimmten Verwaltungsgruppen Firewallregeln hinzufügen, um mehrere Regeln zu verwalten, die dieselben Einflüsse aufweisen.

Im folgenden Beispiel fügen wir der **Telnet-Verwaltung**der Gruppe sowohl eingehende als auch ausgehende Telnet-Firewallregeln hinzu. In Windows PowerShell wird die Gruppenmitgliedschaft beim ersten Erstellen der Regeln angegeben, sodass die vorherigen Beispielregeln neu erstellt werden. Das Hinzufügen von Regeln zu einer benutzerdefinierten Regelgruppe ist in netsh nicht möglich.

Windows PowerShell

```
New-NetFirewallRule -DisplayName “Allow Inbound Telnet” -Direction Inbound -Program
%SystemRoot%\System32\tlntsvr.exe -RemoteAddress LocalSubnet -Action Allow –Group “Telnet Management”
New-NetFirewallRule -DisplayName “Block Outbound Telnet” -Direction Outbound -Program
%SystemRoot%\System32\tlntsvr.exe -RemoteAddress LocalSubnet -Action Allow –Group “Telnet Management”
```

Wenn die Gruppe beim Erstellen der Regel nicht angegeben ist, kann die Regel mithilfe der Punktnotation in Windows PowerShell der Regelgruppe hinzugefügt werden. Sie können die Gruppe nicht angeben `Set-NetFirewallRule` , da mit dem Befehl die Abfrage nach Regelgruppe zulässig ist.

Windows PowerShell

```
$rule = Get-NetFirewallRule -DisplayName “Allow Inbound Telnet”
$rule.Group = “Telnet Management”
$rule | Set-NetFirewallRule
```

Wenn der `Set` Name der Regelgruppe mit dem Befehl angegeben wird, wird die Gruppenmitgliedschaft nicht geändert, sondern alle Regeln der Gruppe erhalten die gleichen Änderungen, die durch die angegebenen Parameter angegeben werden.

Die folgende Scriptlet aktiviert alle Regeln in einer vordefinierten Gruppe, die die Remoteverwaltung beeinflusst, die Firewall-Regeln beeinflusst.

Netsh

```
netsh advfirewall firewall set rule group="Windows Defender Firewall remote management" new enable=yes
```

Windows PowerShell

```
Set-NetFirewallRule -DisplayGroup “Windows Defender Firewall Remote Management” –Enabled True
```

Es gibt auch ein separates `Enable-NetFirewallRule` Cmdlet zum Aktivieren von Regeln nach Gruppe oder nach anderen Eigenschaften der Regel.

Windows PowerShell

```
Enable-NetFirewallRule -DisplayGroup “Windows Defender Firewall Remote Management” -Verbose
```

Löschen einer Firewall-Regel

Regel Objekte können deaktiviert werden, damit Sie nicht mehr aktiv sind. In Windows PowerShell belässt das Cmdlet **Disable-NetFirewallRule** die Regel auf dem System, fügt es aber in einen deaktivierten Zustand ein, damit die Regel nicht mehr angewendet wird und Auswirkungen auf den Datenverkehr hat. Eine deaktivierte Firewall-Regel kann durch **enable-NetFirewallRule**wieder aktiviert werden. Dies unterscheidet sich von der **Remove-NetFirewallRule**, die die Regeldefinition endgültig vom Gerät entfernt.

Das folgende Cmdlet löscht die angegebene vorhandene Firewall-Regel aus dem lokalen Richtlinienspeicher.

Netsh

```
netsh advfirewall firewall delete rule name=“Allow Web 80”
```

Windows PowerShell

```
Remove-NetFirewallRule –DisplayName “Allow Web 80”
```

Wie bei anderen Cmdlets können Sie auch Abfragen, ob Regeln entfernt werden. Hier werden alle Blockierungs Firewall-Regeln vom Gerät gelöscht.

Windows PowerShell

```
Remove-NetFirewallRule –Action Block
```

Beachten Sie, dass es möglicherweise sicherer ist, die Regeln mit dem Befehl **Get** abzufragen und in einer Variablen zu speichern, die Regeln zu beachten, die betroffen sein sollen, und diese dann wie bei den **fest** gelegten Befehlen an den Befehl **Entfernen** weiterleiten. Im folgenden Beispiel wird gezeigt, wie Sie alle Blockierungs Firewall-Regeln anzeigen und dann die ersten vier Regeln löschen können.

Windows PowerShell

```
$x = Get-NetFirewallRule –Action Block
$x
$x[0-3] | Remove-NetFirewallRule
```

Remoteverwaltung

Die Remote Verwaltung mit WinRM ist standardmäßig aktiviert. Die Cmdlets, die den *CimSession* -Parameter unterstützen, verwenden WinRM und können standardmäßig Remote verwaltet werden.

Im folgenden Beispiel werden alle Firewallregeln des beständigen Speichers auf einem Gerät mit dem Namen " **RemoteDevice**" zurückgegeben.

Windows PowerShell

```
Get-NetFirewallRule –CimSession RemoteDevice
```

Wir können alle Änderungen vornehmen oder Regeln auf Remotegeräten anzeigen, indem wir einfach den Parameter – *CimSession* verwenden. Hier wird eine bestimmte Firewall-Regel von einem Remotegerät entfernt.

Windows PowerShell

```
$RemoteSession = New-CimSession –ComputerName RemoteDevice
Remove-NetFirewallRule –DisplayName “AllowWeb80” –CimSession $RemoteSession -Confirm
```

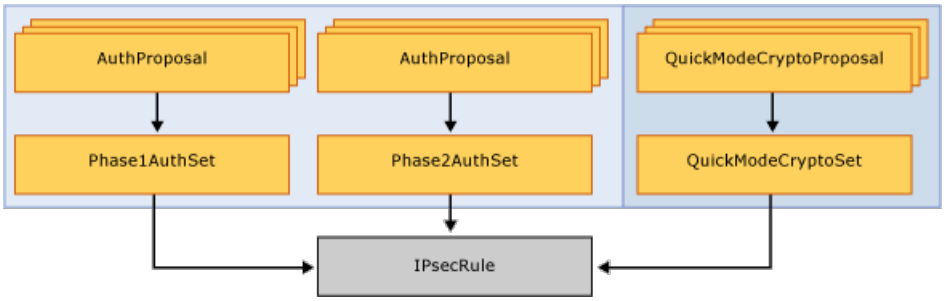
Bereitstellen von grundlegenden IPSec-Regeleinstellungen

Eine IPSec-Richtlinie (Internet Protocol Security) besteht aus Regeln, die das IPSec-Verhalten bestimmen. IPSec unterstützt Peerauthentifizierung auf Netzwerkebene, Datenursprungsauthentifizierung, Datenintegrität, Datenvertraulichkeit (Verschlüsselung) und Wiedergabe-Schutz.

Windows PowerShell kann leistungsfähige, komplexe IPSec-Richtlinien wie in netsh und der Windows Defender-Firewall mit erweiterter Sicherheitskonsole erstellen. Da Windows PowerShell jedoch Objekt basiert ist und nicht

auf Zeichenfolgen-Token basiert, bietet die Konfiguration in Windows PowerShell mehr Kontrolle und Flexibilität.

In netsh wurden die Authentifizierungs-und kryptografischen Sätze als Liste mit durch Kommas getrennten Token in einem bestimmten Format angegeben. In Windows PowerShell erstellen Sie zunächst die gewünschten Authentifizierungs-oder kryptografischen Vorschlags Objekte, anstatt Standardeinstellungen zu verwenden, und bündeln Sie in Listen in Ihrer bevorzugten Reihenfolge. Anschließend erstellen Sie eine oder mehrere IPSec-Regeln, die auf diese Sätze verweisen. Der Vorteil dieses Modells liegt darin, dass der programmgesteuerte Zugriff auf die Informationen in den Regeln viel einfacher ist. Erläutern Sie die folgenden Abschnitte, um Beispiele zu veranschaulichen.



Erstellen von IPSec-Regeln

Mit dem folgenden Cmdlet wird eine grundlegende IPSec-Transportmodus-Regel in einem Gruppenrichtlinienobjekt erstellt. Eine IPSec-Regel ist einfach zu erstellen; Dazu müssen lediglich der Anzeigename und die restlichen Eigenschaften Standardwerte verwendet werden. Der eingehende Datenverkehr wird authentifiziert und die Integrität über die Standardeinstellungen für den Schnellmodus und den Hauptmodus überprüft. Diese Standardeinstellungen finden Sie in der Konsole unter IPsec-Standardeinstellungen anpassen.

Netsh

```
netsh advfirewall set store gpo=domain.contoso.com\gpo_name
netsh advfirewall consec add rule name="Require Inbound Authentication" endpoint1=any endpoint2=any
action=requireinrequestout
```

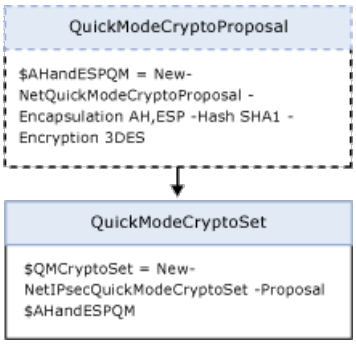
Windows PowerShell

```
New-NetIPsecRule -DisplayName “Require Inbound Authentication” -PolicyStore domain.contoso.com\gpo_name
```

Hinzufügen benutzerdefinierter Authentifizierungsmethoden zu einer IPSec-Regel

Wenn Sie einen benutzerdefinierten Satz von Vorschlägen für den Schnellmodus erstellen möchten, der sowohl AH als auch ESP in einem IPSec-Regelobjekt enthält, erstellen Sie die zugeordneten Objekte separat und verknüpfen deren Zuordnungen. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter auswählen des IPSec-Protokolls .

Sie können dann die neu erstellten benutzerdefinierten Schnellmodus-Richtlinien verwenden, wenn Sie IPSec-Regeln erstellen. Das Verschlüsselungs Satz Objekt ist mit einem IPSec-Regelobjekt verknüpft.



In diesem Beispiel bauen wir auf die zuvor erstellte IPSec-Regel auf, indem Sie einen benutzerdefinierten Schnellmodus-Crypto-Satz angeben. Die endgültige IPSec-Regel setzt voraus, dass der ausgehende Datenverkehr von der angegebenen Kryptographie-Methode authentifiziert wird.

Netsh

```
netsh advfirewall set store gpo=domain.contoso.com\gpo_name
netsh advfirewall consec add rule name="Require Outbound Authentication" endpoint1=any endpoint2=any
action=requireinrequestout qmsecmethods=ah:sha1+esp:sha1-3des
```

Windows PowerShell

```
$AHandESPQM = New-NetIPsecQuickModeCryptoProposal -Encapsulation AH,ESP –AHHash SHA1 -ESPHash SHA1 -Encryption
DES3
$QMCryptoSet = New-NetIPsecQuickModeCryptoSet –DisplayName “ah:sha1+esp:sha1-des3” -Proposal $AHandESPQM –
PolicyStore domain.contoso.com\gpo_name
New-NetIPsecRule -DisplayName “Require Inbound Authentication” -InboundSecurity Require -OutboundSecurity
Request -QuickModeCryptoSet $QMCryptoSet.Name –PolicyStore domain.contoso.com\gpo_name
```

IKEv2-IPSec-Transportregeln

Ein Unternehmensnetzwerk muss möglicherweise die Kommunikation mit einer anderen Agentur sichern. Sie entdecken aber, dass die Agentur nicht-Windows-Betriebssysteme ausführt und die Verwendung des Internet Key Exchange Version2 (IKEv2)-Standards erfordert.

Sie können die IKEv2-Funktionen in Windows Server 2012 nutzen, indem Sie einfach IKEv2 als Schlüsselmodul in einer IPSec-Regel angeben. Dies kann nur mithilfe der Computerzertifikatauthentifizierung erfolgen und kann nicht mit der Phase 2-Authentifizierung verwendet werden.

Windows PowerShell

```
New-NetIPsecRule -DisplayName “Require Inbound Authentication” -InboundSecurity Require -OutboundSecurity
Request –Phase1AuthSet MyCertAuthSet -KeyModule IKEv2 –RemoteAddress $nonWindowsGateway
```

Weitere Informationen zu IKEv2, einschließlich Szenarien, finden Sie unter Sichern von End-to-End-IPSec-Verbindungen mithilfe von IKEv2.

Kopieren einer IPSec-Regel von einer Richtlinie in eine andere

Firewall-und IPSec-Regeln mit denselben Regeleigenschaften können dupliziert werden, um die Aufgabe der erneuten Erstellung in verschiedenen Richtlinien speichern zu vereinfachen.

Wenn Sie die zuvor erstellte Regel aus einem Richtlinienspeicher in einen anderen kopieren möchten, müssen die zugehörigen Objekte ebenfalls separat kopiert werden. Beachten Sie, dass die zugehörigen Firewall-Filter nicht kopiert werden müssen. Sie können Regeln Abfragen, die auf die gleiche Weise wie andere Cmdlets kopiert werden sollen.

Das Kopieren einzelner Regeln ist eine Aufgabe, die über die Netsh-Schnittstelle nicht möglich ist. Hier erfahren Sie, wie Sie es mit Windows PowerShell erreichen.

Windows PowerShell

```
$Rule = Get-NetIPsecRule –DisplayName “Require Inbound Authentication”
$Rule | Copy-NetIPsecRule –NewPolicyStore domain.costoso.com\new_gpo_name
$Rule | Copy-NetPhase1AuthSet –NewPolicyStore domain.costoso.com\new_gpo_name
```

Behandeln von Windows PowerShell-Fehlern

Zum Behandeln von Fehlern in Ihren Windows PowerShell-Skripts können Sie den Parameter *-Error-* Parameter verwenden. Dies ist besonders hilfreich bei den **Remove** -Cmdlets. Wenn Sie eine bestimmte Regel entfernen möchten, werden Sie feststellen, dass Sie fehlschlägt, wenn die Regel nicht gefunden wird. Wenn Regeln entfernt werden, wenn die Regel noch nicht vorhanden ist, ist es im Allgemeinen akzeptabel, diesen Fehler zu ignorieren. In diesem Fall können Sie die folgenden Schritte ausführen, um die Fehler "Regel nicht gefunden" während des Löschvorgangs zu unterdrücken.

Windows PowerShell

```
Remove-NetFirewallRule –DisplayName “Contoso Messenger 98” –ErrorAction SilentlyContinue
```

Beachten Sie, dass durch die Verwendung von Platzhaltern ebenfalls Fehler unterdrückt werden können, die aber möglicherweise Regeln erfüllen, die Sie nicht entfernen wollten. Dies kann eine nützliche Verknüpfung sein, sollte aber nur verwendet werden, wenn Sie wissen, dass es keine zusätzlichen Regeln gibt, die versehentlich gelöscht werden. Das folgende Cmdlet entfernt also auch die Regel und unterdrückt alle Fehler, die nicht gefunden werden.

Windows PowerShell

```
Remove-NetFirewallRule –DisplayName “Contoso Messenger 98*”
```

Wenn Sie Platzhalter verwenden, können Sie den Parameter *-WhatIf* verwenden, wenn Sie die übereinstimmende Regelgruppe überprüfen möchten.

Windows PowerShell

```
Remove-NetFirewallRule –DisplayName “Contoso Messenger 98*” –WhatIf
```

Wenn Sie nur einige der übereinstimmenden Regeln löschen möchten, können Sie den Parameter *– Confirm* verwenden, um eine Bestätigungsaufforderung Regel für Regel abzurufen.

Windows PowerShell

```
Remove-NetFirewallRule –DisplayName “Contoso Messenger 98*” –Confirm
```

Sie können den gesamten Vorgang auch einfach durchführen, indem Sie den Namen jeder Regel anzeigen, während der Vorgang ausgeführt wird.

Windows PowerShell

```
Remove-NetFirewallRule –DisplayName “Contoso Messenger 98*” –Verbose
```

Monitor

Die folgenden Windows PowerShell-Befehle sind im Aktualisierungszyklus einer Bereitstellungsphase hilfreich.

Damit Sie alle IPSec-Regeln in einem bestimmten Store anzeigen können, können Sie die folgenden Befehle verwenden. In netsh zeigt dieser Befehl keine Regeln an, bei denen Profil = Domäne, öffentlich oder Profil = Domäne, privat. Es werden nur Regeln mit der einzelnen Eintrags Domäne angezeigt, die in der Regel enthalten sind. In den folgenden Befehls Beispielen werden die IPSec-Regeln in allen Profilen angezeigt.

Netsh

```
netsh advfirewall consec show rule name=all
```

Windows PowerShell

```
Show-NetIPsecRule –PolicyStore ActiveStore
```

Sie können die Hauptmodus-Sicherheitszuordnungen für Informationen überwachen, wie etwa, welche Peers derzeit mit dem Gerät verbunden sind und welche Schutzsuite für die Bildung der Sicherheitszuordnungen verwendet wird.

Verwenden Sie das folgende Cmdlet, um vorhandene Hauptmodus-Regeln und ihre Sicherheitszuordnungen anzuzeigen:

Netsh

```
netsh advfirewall monitor show mmsa all
```

Windows PowerShell

```
Get-NetIPsecMainModeSA
```

Suchen des Quell-GPO einer Regel

Wenn Sie die Eigenschaften einer bestimmten Regel oder Gruppe von Regeln anzeigen möchten, können Sie die Regel Abfragen. Wenn eine Abfragefelder zurückgibt, die als **NotConfigured**angegeben sind, können Sie ermitteln, von welchem Richtlinienspeicher eine Regel stammt.

Für Objekte, die aus einem Gruppenrichtlinienobjekt stammen (der *-PolicyStoreSourceType-* Parameter wird im Befehl **Show** als **GroupPolicy** angegeben), wird, wenn – *TracePolicyStore* übergeben wird, der Name des Gruppenrichtlinienobjekts gefunden und im ** PolicyStoreSource** -Feld.

Windows PowerShell

```
Get-NetIPsecRule –DisplayName “Require Inbound Authentication” –TracePolicyStore
```

Es ist wichtig zu beachten, dass die offenbarten Quellen keinen Domänennamen enthalten.

Bereitstelleneiner einfachen Domänen Isolierungs Richtlinie

IPSec kann zum Isolieren von Domänenmitgliedern von nicht-Domänenmitgliedern verwendet werden. Bei der Domänenisolierung wird die IPSec-Authentifizierung verwendet, um zu erzwingen, dass die mit der Domäne verbundenen Geräte die Identität der kommunizierenden Geräte positiv festlegen, um die Sicherheit einer Organisation zu verbessern. Eine oder mehrere Features von IPSec können verwendet werden, um den Datenverkehr mit einem IPSec-Regelobjekt zu sichern.

Um die Domänenisolierung in Ihrem Netzwerk zu implementieren, erhalten die Geräte in der Domäne IPSec-Regeln, die unerwünschten eingehenden Netzwerkdatenverkehr blockieren, die nicht durch IPSec geschützt sind. Hier erstellen wir eine IPSec-Regel, die eine Authentifizierung durch Domänenmitglieder erfordert. Dadurch können Sie Domänen verbundene Geräte von Geräten isolieren, die nicht mit einer Domäne verbunden sind. In den folgenden Beispielen wird die Kerberos-Authentifizierung für eingehenden Datenverkehr benötigt und für ausgehenden Datenverkehr angefordert.

Netsh

```
netsh advfirewall set store gpo=domain.contoso.com\domain_isolation
netsh advfirewall consec add rule name=“Basic Domain Isolation Policy” profile=domain endpoint1=”any”
endpoint2=”any” action=requireinrequestout auth1=”computerkerb”
```

Windows PowerShell

```
$kerbprop = New-NetIPsecAuthProposal –Machine –Kerberos
$Phase1AuthSet = New-NetIPsecPhase1AuthSet -DisplayName "Kerberos Auth Phase1" -Proposal $kerbprop –
PolicyStore domain.contoso.com\domain_isolation
New-NetIPsecRule –DisplayName “Basic Domain Isolation Policy” –Profile Domain –Phase1AuthSet
$Phase1AuthSet.Name –InboundSecurity Require –OutboundSecurity Request –PolicyStore
domain.contoso.com\domain_isolation
```

Konfigurieren des IPSec-Tunnelmodus

Mit dem folgenden Befehl wird ein IPSec-Tunnel erstellt, der den Datenverkehr von einem privaten Netzwerk (192.168.0.0/16) über eine Schnittstelle auf dem lokalen Gerät (1.1.1.1), das mit einem öffentlichen Netzwerk verbunden ist, an ein zweites Gerät über dessen öffentliche Schnittstelle (2.2.2.2) an einen anderen privaten Netzwerk (192.157.0.0/16). Der gesamte Datenverkehr über den Tunnel wird mithilfe von ESP/SHA1 auf Integrität überprüft und mithilfe von ESP/DES3 verschlüsselt.

Netsh

```
netsh advfirewall consec add rule name="Tunnel from 192.168.0.0/16 to 192.157.0.0/16" mode=tunnel
endpoint1=192.168.0.0/16 endpoint2=192.157.0.0/16 localtunnelendpoint=1.1.1.1 remotetunnelendpoint=2.2.2.2
action=requireinrequireout qmsecmethods=esp:sha1-3des
```

Windows PowerShell

```
$QMProposal = New-NetIPsecQuickModeCryptoProposal -Encapsulation ESP -ESPHash SHA1 -Encryption DES3
$QMCryptoSet = New-NetIPsecQuickModeCryptoSet –DisplayName “esp:sha1-des3” -Proposal $QMProposal
New-NetIPSecRule -DisplayName “Tunnel from HQ to Dallas Branch” -Mode Tunnel -LocalAddress 192.168.0.0/16 -
RemoteAddress 192.157.0.0/16 -LocalTunnelEndpoint 1.1.1.1 -RemoteTunnelEndpoint 2.2.2.2 -InboundSecurity
Require -OutboundSecurity Require -QuickModeCryptoSet $QMCryptoSet.Name
```

Bereitstellen von sicheren Firewallregeln mit IPSec

In Situationen, in denen nur sicherer Datenverkehr über die Windows Defender-Firewall zugelassen werden kann, ist eine Kombination aus manuell konfigurierten Firewall-und IPSec-Regeln erforderlich. Die Firewallregeln bestimmen die Sicherheitsstufe für zulässige Pakete, und die zugrunde liegenden IPSec-Regeln sichern den Datenverkehr. Die Szenarien können in Windows PowerShell und in netsh ausgeführt werden, mit vielen Ähnlichkeiten bei der Bereitstellung.

Erstellen einer sicheren Firewall-Regel (zulassen, wenn sicher)

Das Konfigurieren der Regel für Firewalls, um Verbindungen zu ermöglichen, wenn Sie sicher sind, erfordert, dass der entsprechende Datenverkehr authentifiziert und Integrität geschützt und dann optional durch IPSec verschlüsselt wird.

Im folgenden Beispiel wird eine Firewall-Regel erstellt, bei der Datenverkehr authentifiziert werden muss. Der Befehl gestattet eingehenden Telnet-Netzwerkdatenverkehr nur, wenn die Verbindung vom Remotegerät mithilfe einer separaten IPSec-Regel authentifiziert wird.

Netsh

```
netsh advfirewall firewall add rule name="Allow Authenticated Telnet" dir=in
program=%SystemRoot%\System32\tlntsvr.exe security=authenticate action=allow
```

Windows PowerShell

```
New-NetFirewallRule -DisplayName “Allow Authenticated Telnet” -Direction Inbound -Program
%SystemRoot%\System32\tlntsvr.exe -Authentication Required -Action Allow
```

Mit dem folgenden Befehl wird eine IPSec-Regel erstellt, die eine erste (Computer-) Authentifizierung erfordert und dann eine optionale zweite (Benutzer-) Authentifizierung versucht. Durch das Erstellen dieser Regel wird der Datenverkehr über die Firewall-Regel Anforderungen für das Messenger-Programm gesichert und ermöglicht.

Netsh

```
netsh advfirewall consec add rule name="Authenticate Both Computer and User" endpoint1=any endpoint2=any
action=requireinrequireout auth1=computerkerb,computerntlm auth2=userkerb,userntlm,anonymous
```

Windows PowerShell

```
$mkerbauthprop = New-NetIPsecAuthProposal -Machine –Kerberos
$mntlmauthprop = New-NetIPsecAuthProposal -Machine -NTLM
$P1Auth = New-NetIPsecPhase1AuthSet -DisplayName “Machine Auth” –Proposal $mkerbauthprop,$mntlmauthprop
$ukerbauthprop = New-NetIPsecAuthProposal -User -Kerberos
$unentlmauthprop = New-NetIPsecAuthProposal -User -NTLM
$anonyauthprop = New-NetIPsecAuthProposal -Anonymous
$P2Auth = New-NetIPsecPhase2AuthSet -DisplayName “User Auth” -Proposal
$ukerbauthprop,$unentlmauthprop,$anonyauthprop
New-NetIPSecRule -DisplayName “Authenticate Both Computer and User” -InboundSecurity Require -OutboundSecurity
Require -Phase1AuthSet $P1Auth.Name –Phase2AuthSet $P2Auth.Name
```

Isolieren eines Servers, indem Verschlüsselung und Gruppenmitgliedschaft erforderlich sind

Um die Sicherheit der Geräte in einer Organisation zu verbessern, können Sie die Domänenisolierung bereitstellen, in der Domänenmitglieder eingeschränkt sind. Sie erfordern Authentifizierung bei der Kommunikation untereinander und ablehnen von nicht authentifizierten eingehenden Verbindungen. Um die Sicherheit von Servern mit vertraulichen Daten zu verbessern, müssen diese Daten geschützt werden, indem der Zugriff nur auf eine Teilmenge von Geräten innerhalb der Unternehmensdomäne zugelassen wird.

IPSec kann diese zusätzliche Schutzebene durch Isolieren des Servers bereitstellen. Bei der Serverisolierung ist der Zugriff auf vertrauliche Daten auf Benutzer und Geräte mit legitimen geschäftlichen Anforderungen beschränkt, und die Daten werden zusätzlich verschlüsselt, um Lauschangriffe zu verhindern.

Erstellen einer Firewall-Regel, die Gruppenmitgliedschaft und-Verschlüsselung erfordert

Zum Bereitstellen der Serverisolierung überlagern wir eine Firewall-Regel, die den Datenverkehr auf autorisierte Benutzer oder Geräte in der IPSec-Regel beschränkt, die die Authentifizierung erzwingt.

Die folgende Firewall-Regel ermöglicht den Telnet-Datenverkehr von Benutzerkonten, die Mitglieder einer benutzerdefinierten Gruppe mit dem Namen "autorisierter Zugriff auf Server" sind. Dieser Zugriff kann aufgrund des Geräts, des Benutzers oder beider Einschränkungen zusätzlich eingeschränkt werden, indem die Einschränkungsparameter angegeben werden.

Eine SDDL-Zeichenfolge (Security Descriptor Definition Language) wird erstellt, indem eine Benutzer-oder Gruppen-Sicherheits-ID (Security Identifier, SID) erweitert wird. Weitere Informationen zum Suchen der SID einer Gruppe finden Sie unter: Suchen der sid für ein Gruppenkonto.

Durch das Einschränken des Zugriffs auf eine Gruppe können Administratoren eine starke

Authentifizierungsunterstützung über die Windows Defender-Firewall und/oder IPSec-Richtlinien erweitern.

Im folgenden Beispiel wird gezeigt, wie Sie eine SDDL-Zeichenfolge erstellen, die Sicherheitsgruppen darstellt.

Windows PowerShell

```
$user = new-object System.Security.Principal.NTAccount (“corp.contoso.com\Administrators”)
$SIDofSecureUserGroup = $user.Translate([System.Security.Principal.SecurityIdentifier]).Value
$secureUserGroup = "D:(A;;CC;;;$SIDofSecureUserGroup)"
```

Mithilfe des vorherigen Scriptlet können Sie auch die SDDL-Zeichenfolge für eine sichere Computergruppe abrufen, wie hier gezeigt:

Windows PowerShell

```
$secureMachineGroup = "D:(A;;CC;;;$SIDofSecureMachineGroup)"
```

Weitere Informationen zum Erstellen von Sicherheitsgruppen oder zum Ermitteln der SDDL-Zeichenfolge finden Sie unter Arbeiten mit SIDs.

Telnet ist eine Anwendung, die keine Verschlüsselung bereitstellt. Diese Anwendung kann Daten wie Namen und Kennwörter über das Netzwerk senden. Diese Daten können von böswilligen Benutzern abgefangen werden. Wenn ein Administrator die Verwendung von Telnet zulassen, aber den Datenverkehr schützen möchte, kann eine Firewall-Regel erstellt werden, die IPSec-Verschlüsselung erfordert. Dies ist erforderlich, damit der Administrator sicher sein kann, dass der gesamte von diesem Port gesendete oder empfangene Datenverkehr verschlüsselt ist, wenn diese Anwendung verwendet wird. Wenn IPSec die Verbindung nicht autorisiert, ist kein Datenverkehr von dieser Anwendung zulässig.

In diesem Beispiel erlauben wir nur authentifizierten und verschlüsselten eingehenden Telnet-Datenverkehr von einer angegebenen sicheren Benutzergruppe durch die Erstellung der folgenden Firewallregel.

Netsh

```
netsh advfirewall set store gpo=domain.contoso.com\Server_Isolation
netsh advfirewall firewall add rule name=“Allow Encrypted Inbound Telnet to Group Members Only”
program=%SystemRoot%\System32\tlntsvr.exe protocol=TCP dir=in action=allow localport=23 security=authenc
rmtusrgrp ="D:(A;;CC;;; S-1-5-21-2329867823-2610410949-1491576313-1735)"
```

Windows PowerShell

```
New-NetFirewallRule -DisplayName "Allow Encrypted Inbound Telnet to Group Members Only" -Program
%SystemRoot%\System32\tlntsvr.exe -Protocol TCP -Direction Inbound -Action Allow -LocalPort 23 -Authentication
Required -Encryption Required –RemoteUser $secureUserGroup –PolicyStore domain.contoso.com\Server_Isolation
```

Endpunkt Sicherheits Erzwingung

Das vorherige Beispiel zeigt die End-to-End-Sicherheit für eine bestimmte Anwendung. In Situationen, in denen die Endpunktsicherheit für viele Anwendungen erforderlich ist, kann eine Firewall-Regel pro Anwendung umständlich und schwierig zu verwalten sein. Die Autorisierung kann die Regel Grundlage überschreiben und auf der IPSec-Ebene ausgeführt werden.

In diesem Beispiel wird die globale IPSec-Einstellung so festgelegt, dass der Verkehr im Transportmodus nur von einer autorisierten Benutzergruppe mit dem folgenden Cmdlet abgerechnet werden kann. Konsultieren Sie die vorherigen Beispiele für das Arbeiten mit Sicherheitsgruppen.

Windows PowerShell

```
Set-NetFirewallSetting -RemoteMachineTransportAuthorizationList $secureMachineGroup
```

Erstellen von Firewallregeln, die IPSec-geschützten Netzwerkverkehr zulassen (authentifizierte Umgehung)

Die authentifizierte Umgehung ermöglicht Datenverkehr von einem bestimmten vertrauenswürdigen Gerät oder Benutzer, Firewall-Blockierungsregeln zu überschreiben. Dies ist hilfreich, wenn ein Administrator Scan Server verwenden möchte, um Geräte zu überwachen und zu aktualisieren, ohne Ausnahmen auf Portebene verwenden zu müssen. Weitere Informationen finden Sie unter Aktivieren der Umgehung authentifizierter Firewalls.

In diesem Beispiel wird davon ausgegangen, dass eine Blockierungs Firewall-Regel vorhanden ist. In diesem Beispiel wird der Netzwerkdatenverkehr an einem beliebigen Port von einer beliebigen IP-Adresse verwendet, um die Blockierungsregel zu überschreiben, wenn der Datenverkehr von einem Gerät oder Benutzerkonto authentifiziert wird, das Mitglied der angegebenen Geräte-oder benutzersicherheitsgruppe ist.

Netsh

```
netsh advfirewall set store gpo=domain.contoso.com\domain_isolation
netsh advfirewall firewall add rule name="Inbound Secure Bypass Rule" dir=in security=authenticate
action="bypass" rmtcomputergrp="D:(A;;CC;;;S-1-5-21-2329867823-2610410949-1491576313-1114)" rmtusrgrp="D:
(A;;CC;;; S-1-5-21-2329867823-2610410949-1491576313-1735)"
```

Windows PowerShell

```
New-NetFirewallRule –DisplayName “Inbound Secure Bypass Rule" –Direction Inbound –Authentication Required –
OverrideBlockRules $true -RemoteMachine $secureMachineGroup –RemoteUser $secureUserGroup –PolicyStore
domain.contoso.com\domain_isolation
```

Zusätzliche Ressourcen

Weitere Informationen zu Windows PowerShell-Konzepten finden Sie unter den folgenden Themen:

- Windows PowerShell-Leitfaden für erste Schritte
- Windows PowerShell-Benutzerhandbuch
- Windows PowerShell zu Hilfethemen
- about_Functions
- about_Functions_Advanced
- about_Execution_Policies
- about_Foreach
- about_Objects
- about_Properties
- about_While
- about_Scripts
- about_Signing
- about_Throw
- about_PSSessions

- about_Modules
- about_Command_Precedence

Windows Defender-Firewall mit erweiterter Sicherheit

01.06.2019 • 8 minutes to read

Entwurfshandbuch

Betrifft

- Windows 10
- Windows Server 2016

Die Windows Defender-Firewall mit erweiterter Sicherheit ist eine Hostfirewall, mit der das Gerät auf zwei Arten gesichert werden kann. Zunächst kann Sie den Netzwerkdatenverkehr filtern, der zum Eingeben des Geräts aus dem Netzwerk zugelassen ist, und außerdem steuern, welchen Netzwerkdatenverkehr das Gerät an das Netzwerk senden darf. Zweitens unterstützt Windows Defender Firewall IPSec, wodurch Sie die Authentifizierung von jedem Gerät aus anfordern können, das versucht, mit Ihrem Gerät zu kommunizieren. Wenn Authentifizierung erforderlich ist, können Geräte, die sich nicht authentifizieren können, nicht mit Ihrem Gerät kommunizieren. Mithilfe von IPSec können Sie auch festlegen, dass ein bestimmter Netzwerkdatenverkehr verschlüsselt wird, um zu verhindern, dass er während der Übertragung zwischen Geräten gelesen oder abgefangen wird.

Die Schnittstelle für die Windows Defender-Firewall ist viel leistungsfähiger und flexibler als die benutzerfreundliche Oberfläche, die in der Windows Defender-Firewall-Systemsteuerung zu finden ist. Beide interagieren mit denselben zugrunde liegenden Diensten, bieten aber unterschiedliche Steuerungsebenen für diese Dienste. Das Windows Defender Firewall Control Panel erfüllt zwar die Anforderungen für den Schutz eines einzelnen Geräts in einer häuslichen Umgebung, bietet jedoch nicht genügend zentralisierte Verwaltungs-oder Sicherheitsfeatures, um einen komplexeren Netzwerkdatenverkehr in einem typischen Unternehmen zu sichern. Unternehmensumgebung.

Weitere Informationen zur Übersicht finden Sie unter Windows Defender-Firewall mit erweiterter Sicherheit.

Informationen zu diesem Leitfaden

Dieser Leitfaden enthält Empfehlungen, mit denen Sie ein Design für die Bereitstellung von Windows Defender Firewall in ihrer Unternehmensumgebung auswählen oder erstellen können. Der Leitfaden beschreibt einige der allgemeinen Ziele für die Verwendung der Windows Defender-Firewall und unterstützt Sie bei der Zuordnung der auf Ihr Szenario anwendbaren Ziele auf die in diesem Leitfaden vorgestellten Designs.

Dieser Leitfaden richtet sich an IT-Experten, denen die Aufgabe zugewiesen wurde, Firewall-und IPSec-Technologien im Netzwerk einer Organisation bereitzustellen, um die Sicherheitsziele der Organisation zu erfüllen.

Die Windows Defender-Firewall sollte Teil einer umfassenden Sicherheitslösung sein, die eine Vielzahl von Sicherheitstechnologien implementiert, wie etwa Umkreisfirewalls, Intrusion Detection Systems, virtuelles privates Netzwerk (VPN), IEEE 802.1 x-Authentifizierung für drahtlose und kabelgebundene Verbindungen sowie Sicherheitsregeln für IPSec-Verbindungen.

Um dieses Handbuch erfolgreich verwenden zu können, benötigen Sie ein gutes Verständnis der Funktionen, die von der Windows Defender-Firewall bereitgestellt werden, und erfahren, wie Sie mithilfe von Gruppenrichtlinien in Active Directory Konfigurationseinstellungen für Ihre verwalteten Geräte übermitteln.

Sie können die Bereitstellungsziele verwenden, um eine dieser Windows Defender-Firewall mit erweiterten Sicherheitsdesigns zu bilden, oder ein benutzerdefiniertes Design, das Elemente aus den hier vorgestellten kombiniert:

- **Grundlegender Firewall-Richtlinienentwurf** Schränkt den Netzwerkverkehr auf und von ihren Geräten

nur auf das ein, was erforderlich und autorisiert ist.

- **Entwurf einer Domänen Isolierungs Richtlinie** Verhindert, dass Geräte, die Domänenmitglieder sind, unerwünschten Netzwerkdatenverkehr von Geräten empfangen, die keine Domänenmitglieder sind. Es können zusätzliche "Zonen" eingerichtet werden, um die speziellen Anforderungen einiger Geräte zu unterstützen, beispielsweise:
  - Eine "Grenz Zone" für Geräte, die Anforderungen von nicht isolierten Geräten empfangen können sollen.
  - Eine "Verschlüsselungszone" für Geräte, die vertrauliche Daten speichern, die während der Netzwerkübertragung geschützt werden müssen.
- **Entwurf der Server Isolierungs Richtlinie** Beschränkt den Zugriff auf einen Server auf eine begrenzte Gruppe von autorisierten Benutzern und Geräten. Wird häufig als Zone in einem Domänen Isolierungs Entwurf konfiguriert, kann aber auch als eigenständiges Design konfiguriert werden und bietet viele Vorteile der Domänenisolierung für eine kleine Gruppe von Geräten.
- **Entwurf einer zertifikatbasierten Isolierungs Richtlinie** Dieses Design ist eine Ergänzung zu den beiden vorherigen Entwürfen und unterstützt alle ihre Funktionen. Anstelle der standardmäßig in Active Directory verwendeten KerberosV5-Authentifizierung werden kryptografische Zertifikate verwendet, die für die Authentifizierung auf Clients und Servern bereitgestellt werden. Auf diese Weise können Geräte, die nicht zu einer Active Directory-Domäne gehören, wie Geräte, auf denen andere Betriebssysteme als Windows ausgeführt werden, an ihrer Isolierungslösung teilnehmen.

Neben Beschreibungen und Beispiel für jedes Design finden Sie Richtlinien für das Sammeln erforderlicher Daten zu Ihrer Umgebung. Sie können diese Richtlinien dann verwenden, um Ihre Windows Defender-Firewall mit Advanced Security Deployment zu planen und zu entwerfen. Nachdem Sie dieses Handbuch gelesen und die Anforderungen Ihrer Organisation gesammelt, dokumentiert und zugeordnet haben, verfügen Sie über die Informationen, die Sie benötigen, um mit der Bereitstellung von Windows Defender Firewall mithilfe der Anleitungen in der Windows Defender-Firewall mit Advanced zu beginnen. Leitfaden zur Sicherheits Bereitstellung.

Sie finden die Windows Defender-Firewall mit Advanced Security Deployment Guide an diesen Speicherorten:

- Windows Defender-Firewall mit erweitertem Sicherheits Bereitstellungshandbuch
- (Herunterladbares Word-Dokument)

In diesem Abschnitt

THEMA	BESCHREIBUNG
Grundlegendes zur Windows Defender-Firewall mit erweitertem Sicherheitsentwurfsprozess	Hier erfahren Sie, wie Sie mit der Windows Defender-Firewall mit erweitertem Sicherheitsdesign Verfahren beginnen.
Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen	Erfahren Sie, wie Sie Ihre Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen identifizieren.
Zuordnen Ihrer Bereitstellungsziele zu einer Windows Defender-Firewall mit erweitertem Sicherheits Design	Nachdem Sie die Überprüfung der vorhandenen Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen abgeschlossen haben und feststellen, welche Ziele für Ihre spezifische Bereitstellung wichtig sind, können Sie diese Ziele einer bestimmten Windows Defender-Firewall mit erweiterten Sicherheitsentwurf.

THEMA	BESCHREIBUNG
Auswerten der Windows Defender-Firewall mit erweiterten Sicherheitsentwurfs Beispielen	Erfahren Sie, wie Sie die Windows Defender-Firewall verwenden, um die Sicherheit der Computer zu verbessern, die mit dem Netzwerk verbunden sind.
Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategie	Wenn Sie das effektivste Design für den Schutz des Netzwerks auswählen möchten, müssen Sie Zeit damit verbringen, wichtige Informationen zu Ihrer aktuellen Computerumgebung zu sammeln.
Planen der Windows Defender-Firewall mit erweitertem Sicherheits Design	Nachdem Sie die relevanten Informationen in den vorherigen Abschnitten gesammelt und die Grundlagen der Entwürfe verstanden haben, wie weiter oben in diesem Leitfaden beschrieben, können Sie das Design (oder die Kombination von Designs) auswählen, das Ihren Anforderungen entspricht.
AnhangA: GPO-Beispielvorlagendateien für die in diesem Handbuch verwendeten Einstellungen	Sie können eine XML-Datei mit angepassten Registrierungseinstellungen in ein Gruppenrichtlinienobjekt (GPO) importieren, indem Sie das Feature Einstellungen der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) verwenden.

In diesem Leitfaden verwendete Terminologie

In der folgenden Tabelle werden die in diesem Leitfaden verwendeten Begriffe identifiziert und definiert.

BEGRIFF	DEFINITION
Active Directory-Domäne	Eine Gruppe von Geräten und Benutzern, die von einem Administrator mithilfe von Active Directory-Domänendiensten verwaltet werden (hinzugefügt). Geräte in einer Domäne verwenden eine gemeinsame Verzeichnisdatenbank und Sicherheitsrichtlinien. Mehrere Domänen können in einer "Gesamtstruktur koexistieren," wobei Vertrauensstellungen die Gesamtstruktur als Sicherheitsgrenze festlegen.
Authentifizierung	Ein Prozess, mit dem der Absender einer Nachricht seine Identität für den Empfänger nachweisen kann. Für die Verbindungssicherheit in Windows wird die Authentifizierung von der IPSec-Protokoll Suite implementiert.
Grenzbereich	Eine Teilmenge der Geräte in einer isolierten Domäne, die in der Lage sein müssen, unerwünschten und nicht authentifizierten Netzwerkdatenverkehr von Geräten zu empfangen, die nicht Mitglieder der isolierten Domäne sind. Geräte in der Grenzzonen Anforderung, aber keine Authentifizierung erforderlich. Sie verwenden IPSec für die Kommunikation mit anderen Geräten in der isolierten Domäne.
Verbindungssicherheitsregel	Eine Regel in der Windows Defender-Firewall, die eine Reihe von Bedingungen und eine Aktion enthält, die auf Netzwerkpakete angewendet werden soll, die den Bedingungen entsprechen. Mit der Aktion kann das Paket zugelassen, das Paket blockiert oder das Paket durch IPSec geschützt werden. In früheren Versionen von Windows wurde dies als IPSec- *Regel*bezeichnet.

BEGRIFF	DEFINITION
Zertifikatbasierte Isolierung	Eine Möglichkeit zum Hinzufügen von Geräten, die die KerberosV5-Authentifizierung nicht für eine isolierte Domäne verwenden, mithilfe einer alternativen Authentifizierungsmethode. Jedes Gerät in der isolierten Domäne und die Geräte, die KerberosV5 nicht verwenden können, werden mit einem Gerätezertifikat bereitgestellt, das zur Authentifizierung untereinander verwendet werden kann. Die zertifikatbasierte Isolierung erfordert eine Möglichkeit, ein geeignetes Zertifikat zu erstellen und zu verteilen (wenn Sie sich entscheiden, keines von einem kommerziellen Zertifikatanbieter zu kaufen).
Domänenisolierung	Eine Methode, mit der Sie die Geräte in einer Organisation schützen können, indem Sie die Identität der anderen Geräte vor dem Austausch von Informationen authentifizieren und Verbindungsanforderungen von Geräten ablehnen, die sich nicht authentifizieren können. Die Domänenisolierung nutzt die Active Directory-Domänenmitgliedschaft und das KerberosV5-Authentifizierungsprotokoll, das allen Mitgliedern der Domäne zur Verfügung steht. Siehe "auch isolierte" Domäne in dieser Tabelle.
Verschlüsselungszone	Eine Teilmenge der Geräte in einer isolierten Domäne, die vertrauliche Daten verarbeiten. Geräte, die Teil des Verschlüsselungs Bereichs sind, haben den gesamten Netzwerkverkehr verschlüsselt, um zu verhindern, dass nicht autorisierte Benutzer Sie anzeigen können. Geräte, die Teil des Verschlüsselungs Bereichs sind, unterliegen in der Regel auch den Zugriffs Steuerungs Einschränkungen der Serverisolierung.
Firewall-Regel	Eine Regel in der Windows Defender-Firewall, die eine Reihe von Bedingungen enthält, die verwendet werden, um zu ermitteln, ob ein Netzwerkpaket die Firewall durchlaufen darf. Standardmäßig blockieren die Firewallregeln in Windows Server 2012, Windows Server2008R2, Windows Server2008, Windows 8, Windows7 und Windows Vista unerwünschten eingehenden Netzwerkdatenverkehr. Ebenso ist standardmäßig der gesamte ausgehende Netzwerkdatenverkehr zulässig. Die in früheren Versionen von Windows enthaltene Firewall hat nur eingehenden Netzwerkdatenverkehr gefiltert.
IPSec (Internet Protocol Security)	Eine Reihe von branchenüblichen, auf Kryptographie basierenden Schutzdiensten und-Protokollen. IPSec schützt alle Protokolle in der TCP/IP-Protokoll Suite mit Ausnahme von ARP (Address Resolution Protocol).
IPSec-Richtlinie	Eine Sammlung von Verbindungssicherheitsregeln, die den erforderlichen Schutz für den Netzwerkdatenverkehr bieten, der das Gerät eingibt und verlässt. Der Schutz umfasst die Authentifizierung des sendenden und empfangenden Geräts, den Integritätsschutz des zwischen Ihnen ausgetauschten Netzwerkverkehrs und kann die Verschlüsselung umfassen.

BEGRIFF	DEFINITION
Isolierte Domäne	Eine Active Directory-Domäne (oder eine Active Directory-Gesamtstruktur oder eine Gruppe von Domänen mit bidirektionalen Vertrauensstellungen), auf die Gruppenrichtlinieneinstellungen angewendet werden, um Ihre Mitglieds Geräte mithilfe von IPsec-Verbindungssicherheitsregeln zu schützen. Mitglieder der isolierten Domäne erfordern Authentifizierung für alle nicht angeforderten eingehenden Verbindungen (mit Ausnahmen, die von den anderen Zonen behandelt werden). In diesem Leitfaden bezieht sich der Begriff *isolierte Domäne* auf das IPSec-Konzept einer Gruppe von Geräten, die die Authentifizierung freigeben können. Der Begriff *Active Directory-Domäne* bezieht sich auf die Gruppe von Geräten, die eine Sicherheitsdatenbank mithilfe von Active Directory freigeben.
Server Isolierung	Eine Methode für die Verwendung von Gruppenmitgliedschaften, um den Zugriff auf einen Server zu beschränken, der in der Regel bereits Mitglied einer isolierten Domäne ist. Der zusätzliche Schutz beruht auf der Verwendung der Authentifizierungsanmeldeinformationen des anfordernden Geräts, um die Gruppenmitgliedschaft zu ermitteln, und dann nur, wenn das Computerkonto (und optional das Benutzerkonto) Mitglied einer autorisierten Gruppe ist.
Angeforderter Netzwerkdatenverkehr	Netzwerkdatenverkehr, der als Antwort auf eine Anforderung gesendet wird. Standardmäßig ermöglicht die Windows Defender-Firewall alle angeforderten Netzwerkdatenverkehr durch.
Unangeforderter Netzwerkdatenverkehr	Netzwerkdatenverkehr, bei dem es sich nicht um eine Antwort auf eine frühere Anforderung handelt, und die vom empfangenden Gerät nicht unbedingt vorweggenommen werden kann. Standardmäßig blockiert die Windows Defender-Firewall alle unerwünschten Netzwerkdatenverkehr.
Zone	Eine Zone ist eine logische Gruppierung von Geräten, die aufgrund ihrer Kommunikationsanforderungen allgemeine IPSec-Richtlinien freigeben. Die Grenz Zone ermöglicht beispielsweise eingehende Verbindungen von nicht vertrauenswürdigen Geräten. Für den Verschlüsselungsbereich müssen alle Verbindungen verschlüsselt werden. Dies bezieht sich nicht auf die Term Zone, wie Sie von Domain Name System (DNS) verwendet wird.

Nächster Schritt: Grundlegendes zur Windows Defender-Firewall mit erweitertem Sicherheitsentwurfsprozess

Grundlegendes zur Windows Defender-Firewall mit erweitertem Sicherheitsentwurfsprozess

04.12.2019 • 2 minutes to read

Das Entwerfen einer beliebigen Bereitstellung beginnt mit der Durchführung mehrerer wichtiger Aufgaben:

- Identifizieren Ihrer Windows Defender-Firewall mit erweiterten Sicherheits Design Zielen
- Zuordnen Ihrer Bereitstellungsziele zu einer Windows Defender-Firewall mit erweitertem Sicherheits Design
- Auswerten der Windows Defender-Firewall mit erweiterten Sicherheitsentwurfs Beispielen

Nachdem Sie ihre Bereitstellungsziele identifiziert und einer Windows Defender-Firewall mit erweitertem Sicherheitsdesign zugeordnet haben, können Sie mit der Dokumentierung des Entwurfs beginnen, basierend auf den Prozessen, die in den folgenden Themen beschrieben werden:

- Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategie
- Planen der Windows Defender-Firewall mit erweitertem Sicherheits Design

Weiter: Identifizieren Ihrer Windows Defender-Firewall mit erweiterten Sicherheits Design Zielen

Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Die ordnungsgemäße Identifizierung Ihrer Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen ist für den Erfolg Ihres Windows Defender-Firewall-Entwurfsprojekts von entscheidender Bedeutung. Bilden Sie ein Projektteam, das Bereitstellungsprobleme in einer Visions Aussage deutlich artikulieren kann. Wenn Sie Ihre Vision-Anweisung schreiben, identifizieren, klären und verfeinern Sie ihre Bereitstellungsziele. Priorisieren und, wenn möglich, kombinieren Sie ihre Bereitstellungsziele, damit Sie Windows Defender Firewall mithilfe eines iterativen Ansatzes entwerfen und bereitstellen können. Sie können die vordefinierten Windows Defender-Firewall-Bereitstellungsziele nutzen, die in diesem Leitfaden für Ihre Szenarios relevant sind.

In der folgenden Tabelle sind die drei Hauptaufgaben für das artikulieren, verfeinern und anschließende Dokumentieren der Bereitstellungsziele für Windows Defender-Firewall aufgeführt:

BEREITSTELLUNGSZIEL AUFGABEN	VERWEISLINKS
Bewerten Sie die vordefinierte Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen, die in diesem Abschnitt des Leitfadens bereitgestellt werden, und kombinieren Sie mindestens ein Ziel, um Ihre organisatorischen Ziele zu erreichen.	Vordefinierte Bereitstellungsziele: • Schützen von Geräten vor unerwünschtem Netzwerkverkehr • Beschränken des Zugriffs auf vertrauenswürdige Geräte • Vorschreiben der Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen • Einschränken des Zugriffs auf vertrauliche Ressourcen auf bestimmte Benutzer oder Geräte
Zuordnen eines Ziels oder einer Kombination der vordefinierten Bereitstellungsziele zu einer vorhandenen Windows Defender-Firewall mit erweitertem Sicherheitsdesign	• Zuordnen Ihrer Bereitstellungsziele zu einer Windows Defender-Firewall mit erweitertem Sicherheits Design
Dokumentieren Sie basierend auf dem Status Ihrer aktuellen Infrastruktur ihre Bereitstellungsziele für Ihre Windows Defender-Firewall mit erweitertem Sicherheitsdesign in einem Bereitstellungsplan.	• Entwerfen einer Windows Defender-Firewall-Strategie • Planen Ihres Windows Defender-Firewall-Designs mit erweiterter Sicherheit

Nächstes: Schützen von Geräten vor unerwünschtem Netzwerkdatenverkehr

Schützen von Geräten vor unerwünschtem Netzwerkverkehr

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Obwohl Netzwerkumkreisfirewalls wichtigen Schutz für Netzwerkressourcen vor externen Bedrohungen bieten, gibt es Netzwerkbedrohungen, die von einer Umkreisfirewall nicht geschützt werden können. Einige Angriffe könnten erfolgreich in die Umkreisfirewall eindringen, und was kann Sie an diesem Punkt verhindern? Andere Angriffe können aus dem Netzwerk stammen, wie etwa Malware, die auf tragbaren Medien eingebracht und auf einem vertrauenswürdigen Gerät ausgeführt wird. Tragbare Geräte werden häufig außerhalb des Netzwerks aufgenommen und direkt mit dem Internet verbunden, ohne dass ein ausreichender Schutz zwischen dem Gerät und Sicherheitsbedrohungen besteht.

Berichte über gezielte Angriffe auf Organisationen, Regierungen und Einzelpersonen haben sich in den letzten Jahren weiter verbreitet. Eine allgemeine Übersicht über diese Bedrohungen, auch bekannt als erweiterte persistent Threats (APT), finden Sie im Microsoft Security Intelligence-Bericht.

Das Ausführen einer hostbasierten Firewall auf allen Geräten, die von Ihrer Organisation verwaltet werden, ist eine wichtige Ebene in einer "Tiefenverteidigungsstrategie". Eine hostbasierte Firewall schützt vor Angriffen, die aus dem Netzwerk stammen, und bietet auch zusätzlichen Schutz vor Angriffen von außerhalb des Netzwerks, die das Eindringen in die Umkreisfirewall verwalten. Außerdem reist Sie mit einem tragbaren Gerät, um den Schutz zu gewährleisten, wenn Sie sich nicht im Netzwerk der Organisation befindet.

Eine hostbasierte Firewall hilft, ein Gerät zu sichern, indem der gesamte Netzwerkdatenverkehr abgesetzt wird, der nicht dem vom Administrator entworfenen Regelsatz für zulässigen Netzwerkdatenverkehr entspricht. Dieses Design, das dem Standardentwurf für Firewall-Richtlinienentspricht, bietet die folgenden Vorteile:

- Netzwerkdatenverkehr, der eine Antwort auf eine Anforderung vom lokalen Gerät ist, ist in das Gerät aus dem Netzwerk zulässig.
- Der nicht angeforderte Netzwerkdatenverkehr, der aber mit einer Regel für zulässigen Netzwerkdatenverkehr übereinstimmt, ist vom Netzwerk aus auf das Gerät zugelassen.

  Woodgrove Bank möchte beispielsweise, dass ein Gerät, auf dem SQL Server ausgeführt wird, die von Clientgeräten gesendeten SQL-Abfragen empfangen kann. Die auf dem Gerät, auf dem SQL Server ausgeführt wird, enthaltene Firewall-Richtlinie enthält Firewallregeln, mit denen der eingehende Netzwerkdatenverkehr für das SQL Server-Programm ausdrücklich zugelassen wird.
- Der nicht ausdrücklich blockierte ausgehende Netzwerkdatenverkehr ist im Netzwerk zulässig.

  Die Woodgrove Bank verfügt beispielsweise über eine Unternehmensrichtlinie, die die Verwendung bestimmter Peer-to-Peer-Dateifreigabeprogramme untersagt. Die Firewall-Richtlinie, die auf den Computern im Netzwerk bereitgestellt wird, enthält Firewallregeln, die den eingehenden und ausgehenden Netzwerkdatenverkehr für die verbotenen Programme blockieren. Alle anderen ausgehenden Datenverkehr ist zulässig.

Die folgende Komponente wird für dieses Bereitstellungsziel empfohlen:

- **Active Directory**: Active Directory unterstützt die zentralisierte Verwaltung von

Verbindungssicherheitsregeln, indem die Regeln in einem oder mehreren Gruppenrichtlinienobjekten (Group Policy Objects, GPOs) konfiguriert werden, die automatisch auf alle relevanten Computer in der Domäne angewendet werden können.

Andere Methoden zum Bereitstelleneiner Firewall-Richtlinie stehen zur Verfügung, beispielsweise das Erstellen von Skripts, die das Netsh-Befehlszeilentool verwenden, und das anschließende Ausführen dieser Skripts auf jedem Computer in der Organisation. In diesem Leitfaden wird Active Directory als empfohlene Methode für die Bereitstellung verwendet, da es sich auf sehr große Organisationen skalieren kann.

Nächster Schritt: Einschränken des Zugriffs auf nur vertrauenswürdige Geräte

Beschränken des Zugriffs auf vertrauenswürdige Geräte

07.08.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

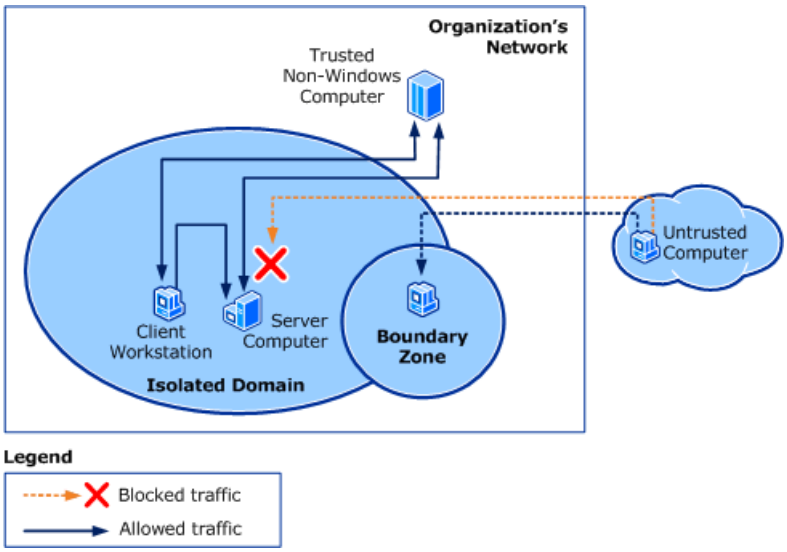
Ihr Unternehmensnetzwerk hat wahrscheinlich eine Verbindung mit dem Internet. Sie haben wahrscheinlich auch Partner, Anbieter oder Auftragnehmer, die Geräte, die nicht im Besitz Ihrer Organisation sind, an Ihr Netzwerk anhängen. Da Sie diese Geräte nicht verwalten, können Sie Ihnen nicht vertrauen, dass Sie frei von bösartiger Software sind, mit den neuesten Sicherheitsupdates verwaltet werden oder in irgendeiner Weise mit den Sicherheitsrichtlinien Ihrer Organisation in Einklang stehen. Diese nicht vertrauenswürdigen Geräte sowohl auf als auch außerhalb Ihres physikalischen Netzwerks dürfen nicht auf die Geräte Ihrer Organisation zugreifen, es sei denn, es ist wirklich erforderlich.

Um dieses Risiko zu verringern, müssen Sie in der Lage sein, die vertrauenswürdigen Geräte zu isolieren und deren Fähigkeit, unerwünschten Netzwerkdatenverkehr von nicht vertrauenswürdigen Geräten zu empfangen, zu beschränken. Mithilfe der Verbindungssicherheit und Firewallregeln, die in der Windows Defender-Firewall mit erweiterter Sicherheit zur Verfügung stehen, können Sie die vertrauenswürdigen Geräte logisch isolieren, indem Sie festlegen, dass der gesamte nicht angeforderte eingehende Netzwerkdatenverkehr authentifiziert werden soll. Die Authentifizierung stellt sicher, dass sich jedes Gerät oder jeder Benutzer mithilfe von Anmeldeinformationen, die vom anderen Gerät als vertrauenswürdig eingestuft werden, positiv identifizieren kann. Verbindungssicherheitsregeln können so konfiguriert werden, dass Sie IPSec mit dem in Active Directory verfügbaren KerberosV5-Protokoll verwenden, oder Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle als Authentifizierungsmethode ausgestellt wurden.

> **Hinweis:** da die primäre Authentifizierungsmethode für Geräte, auf denen Windows ausgeführt wird, die Verwendung des KerberosV5-Protokolls mit der Mitgliedschaft in einer Active Directory-Domäne empfiehlt, bezieht sich dieser Leitfaden auf diese logische Trennung von Computern als * Domänenisolierung*, auch wenn Zertifikate verwendet werden, um den Schutz auf Geräte zu erweitern, die nicht Teil einer Active Directory-Domäne sind.

Der von der Domänenisolierung bereitgestellte Schutz kann Ihnen dabei helfen, behördliche und Legislative Anforderungen zu erfüllen, wie Sie beispielsweise im Federal Information Security Management Act von 2002 (FISMA), dem Sarbanes-Oxley-Act von 2002, der Portabilität von Krankenkassen zu finden sind. und Verantwortlichkeits Akt von 1996 (HIPAA) sowie andere behördliche und Branchen rechtliche Bestimmungen.

Die folgende Abbildung zeigt eine isolierte Domäne mit einer der Zonen, die optional Teil des Entwurfs sind. Die Regeln, die sowohl die isolierte Domäne als auch die verschiedenen Zonen implementieren, werden mithilfe von Gruppenrichtlinien und Active Directory bereitgestellt.



Diese Ziele, die dem Design der Domänen Isolierungs Richtlinien und dem Entwurf einer zertifikatbasierten Isolierungs Richtlinieentsprechen, bieten die folgenden Vorteile:

- Geräte in der isolierten Domäne akzeptieren unerwünschten eingehenden Netzwerkdatenverkehr nur, wenn Sie von einem anderen Gerät in der isolierten Domäne authentifiziert werden können. Ausnahmeregeln können definiert werden, um eingehenden Datenverkehr von vertrauenswürdigen Computern zuzulassen, die IPSec-Authentifizierung aus irgendeinem Grund nicht durchführen können.

  Woodgrove Bank möchte beispielsweise, dass alle Ihre Geräte alle unerwünschten eingehenden Netzwerkdatenverkehr von jedem Gerät blockieren, das nicht verwaltet wird. Die Verbindungssicherheitsregeln, die für Domänenmitglieds Geräte bereitgestellt werden, erfordern die Authentifizierung als Domänenmitglied oder mithilfe eines Zertifikats, bevor ein Unaufgefordertes eingehendes Netzwerkpaket akzeptiert wird.

- Geräte in der isolierten Domäne können weiterhin ausgehenden Netzwerkdatenverkehr an nicht vertrauenswürdige Geräte senden und die Antworten auf ausgehende Anforderungen empfangen.

  Die Woodgrove Bank möchte beispielsweise, dass Ihre Benutzer auf Clientgeräten auf Websites im Internet zugreifen können. Dies ist in den Standardeinstellungen für Windows Defender-Firewalls für ausgehenden Netzwerkdatenverkehr möglich. Es sind keine weiteren Regeln erforderlich.

Diese Ziele unterstützen auch optionale Zonen, die erstellt werden können, um einen benutzerdefinierten Schutz hinzuzufügen, der den Anforderungen von Teilmengen der Geräte einer Organisation entspricht:

- Geräte in der "Grenz Zone" sind für die Verwendung von Verbindungssicherheitsregeln konfiguriert, die eine Authentifizierung anfordern, aber nicht erforderlich sind. Auf diese Weise können Sie unerwünschten eingehenden Netzwerkdatenverkehr von nicht vertrauenswürdigen Geräten empfangen und auch Datenverkehr von den anderen Mitgliedern der isolierten Domäne empfangen.

  Beispielsweise verfügt die Woodgrove Bank über einen Server, auf den die Geräte ihrer Partner über das Internet zugreifen müssen. Die Regeln, die auf Geräte in der Grenz Zone angewendet werden, verwenden die Authentifizierung, wenn das Clientgerät Sie unterstützenkann, aber blockieren Sie die Verbindung nicht, wenn sich das Clientgerät nicht authentifizieren kann.

- Für Geräte im Bereich "Verschlüsselung" muss der gesamte Netzwerkdatenverkehr verschlüsselt werden, um potenziell sensibles Material zu sichern, wenn es über das Netzwerk gesendet wird.

  Die Woodgrove Bank möchte beispielsweise, dass die Geräte, auf denen SQL Server ausgeführt wird, nur Daten übertragen, die verschlüsselt sind, um die auf diesen Geräten gespeicherten vertraulichen Daten zu schützen.

Für dieses Bereitstellungsziel sind die folgenden Komponenten erforderlich:

- **Active Directory**: Active Directory unterstützt die zentralisierte Verwaltung von Verbindungssicherheitsregeln durch Konfigurieren der Regeln in einem oder mehreren GPOs, die automatisch auf alle relevanten Geräte in der Domäne angewendet werden können.

Nächster Schritt: Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen erforderlich

Vorschreiben der Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen

07.08.2019 • 2 minutes to read

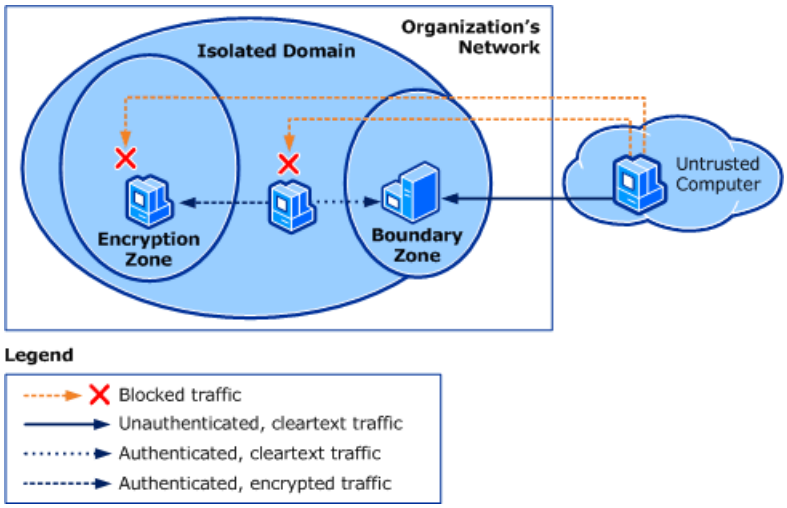
Betrifft

- Windows 10
- Windows Server 2016

Durch die Verwendung der Authentifizierung im zuvor beschriebenen Ziel (Einschränken des Zugriffs auf nur vertrauenswürdige Geräte) kann ein Gerät in der isolierten Domäne den Datenverkehr von nicht vertrauenswürdigen Geräten blockieren. Es verhindert jedoch nicht, dass ein nicht vertrauenswürdiges Gerät den von zwei vertrauenswürdigen Geräten freigegebenen Netzwerkdatenverkehr ablauscht, weil Netzwerkpakete standardmäßig nicht verschlüsselt sind.

Bei Geräten, die vertrauliche Informationen über das Netzwerk freigeben, können Sie mit der Windows Defender-Firewall mit erweiterter Sicherheit festlegen, dass alle derartigen Netzwerkdatenverkehr verschlüsselt werden. Die Verwendung von Verschlüsselung kann Ihnen helfen, behördliche und Legislative Anforderungen zu erfüllen, wie Sie im Federal Information Security Management Act von 2002 (FISMA), dem Sarbanes-Oxley-Act von 2002, dem Sozialversicherungs-und Verantwortlichkeits Gesetz von 1996 (HIPAA) und andere behördliche und Branchen rechtliche Bestimmungen. Durch das Erstellen von Verbindungssicherheitsregeln, die für Geräte gelten, die vertrauliche Daten hosten und austauschen, können Sie die Vertraulichkeit dieser Daten schützen, indem Sie Sie verschlüsseln.

Die folgende Abbildung zeigt eine Verschlüsselungszone in einer isolierten Domäne. Die Regeln, die sowohl die isolierte Domäne als auch die verschiedenen Zonen implementieren, werden mithilfe von Gruppenrichtlinien und Active Directory bereitgestellt.



Dieses Ziel bietet die folgenden Vorteile:

- Geräte im Verschlüsselungsbereich erfordern eine Authentifizierung für die Kommunikation mit anderen Geräten. Dies funktioniert nicht anders als das Ziel und Design der Domänenisolierung. Weitere Informationen finden Sie unter Einschränken des Zugriffs auf nur vertrauenswürdige Geräte.
- Für Geräte im Verschlüsselungsbereich müssen alle eingehenden und ausgehenden Netzwerkdatenverkehr verschlüsselt werden.

  Die Woodgrove Bank verarbeitet beispielsweise vertrauliche Kundendaten auf einem Gerät, das vor

Lauschangriffen durch Geräte im Netzwerk geschützt werden muss. Verbindungssicherheitsregeln geben an, dass der gesamte Datenverkehr durch einen hinreichend komplexen Verschlüsselungsalgorithmus verschlüsselt werden muss, um den Datenschutz zu gewährleisten.

- Geräte im Verschlüsselungsbereich sind häufig gute Kandidaten für die Serverisolierung, wobei der Zugriff auf Computerkonten und Benutzerkonten begrenzt ist, die Mitglieder einer autorisierten Zugriffsgruppe sind. In vielen Organisationen sind die Verschlüsselungszone und der Server Isolationsbereich identisch. Weitere Informationen finden Sie unter Einschränken des Zugriffs auf bestimmte Benutzer oder Geräte.

Für dieses Bereitstellungsziel sind die folgenden Komponenten erforderlich:

- **Active Directory**: Active Directory unterstützt die zentralisierte Verwaltung von Verbindungssicherheitsregeln durch Konfigurieren der Regeln in einem oder mehreren GPOs, die automatisch auf alle relevanten Geräte in der Domäne angewendet werden können.

Nächster Schritt: Einschränken des Zugriffs auf bestimmte Benutzer oder Geräte

Beschränken des Zugriffs auf bestimmte Benutzer oder Computer

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

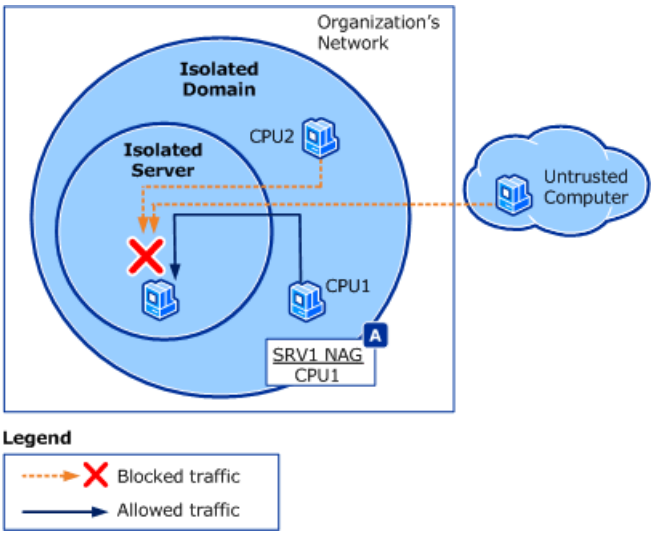
Die Domänenisolierung (wie im vorhergehenden Ziel beschriebene beschränken des Zugriffs auf vertrauenswürdige Geräte) verhindert, dass Geräte, die Mitglieder der isolierten Domäne sind, den Netzwerkdatenverkehr von nicht vertrauenswürdigen Geräten akzeptieren. Einige Geräte im Netzwerk können jedoch vertrauliche Daten hosten, die zusätzlich auf die Benutzer und Computer beschränkt sein müssen, die über eine geschäftliche Anforderung für den Zugriff auf die Daten verfügen.

Mit der Windows Defender-Firewall mit erweiterter Sicherheit können Sie den Zugriff auf Geräte und Benutzer einschränken, die Mitglieder von Domänengruppen sind, die für den Zugriff auf dieses Gerät autorisiert sind. Diese Gruppen werden als *Netzwerkzugriffsgruppen*bezeichnet. Wenn sich ein Gerät bei einem Server authentifiziert, überprüft der Server die Gruppenmitgliedschaft des Computerkontos und des Benutzerkontos und gewährt nur Zugriff, wenn die Mitgliedschaft im nag bestätigt wird. Durch Hinzufügen dieser Prüfung wird eine virtuelle "sichere Zone" innerhalb des Domänen Isolations Bereichs erstellt. Sie können mehrere Geräte in einer einzigen sicheren Zone haben, und es ist wahrscheinlich, dass Sie eine separate Zone für jede Gruppe von Servern erstellen, die bestimmte Sicherheitszugriffs Anforderungen aufweisen. Geräte, die Teil dieser Server Isolations Zone sind, sind häufig auch Teil des Verschlüsselungs Bereichs (siehe anfordern von Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen).

Das Einschränken des Zugriffs auf nur Benutzer und Geräte, die über eine geschäftliche Anforderung verfügen, kann Ihnen helfen, behördliche und Legislative Anforderungen zu erfüllen, wie Sie im Federal Information Security Management Act von 2002 (FISMA), dem Sarbanes-Oxley Act von 2002, enthalten sind. Das Krankenversicherungs-und Verantwortlichkeits Gesetz von 1996 (HIPAA) sowie andere behördliche und Branchen rechtliche Bestimmungen.

Sie können den Zugriff einschränken, indem Sie entweder Computer-oder Benutzeranmeldeinformationen angeben.

Die folgende Abbildung zeigt einen isolierten Server und Beispiele für Geräte, die mit ihr kommunizieren können und können. Geräte, die sich außerhalb des Woodgrove-Unternehmensnetzwerks befinden, oder Computer, die sich in der isolierten Domäne befinden, aber nicht Mitglieder des erforderlichen nag sind, können nicht mit dem isolierten Server kommunizieren.



Dieses Ziel, das dem Design der Server Isolierungs Richtlinieentspricht, bietet die folgenden Features:

- Isolierte Server akzeptieren unerwünschten eingehenden Netzwerkdatenverkehr nur von Geräten oder Benutzern, die Mitglieder des nag sind.
- Isolierte Server können als Teil einer isolierten Domäne implementiert und als eine andere Zone behandelt werden. Mitglieder der Zonengruppe erhalten ein GPO mit Regeln, die eine Authentifizierung erfordern, und geben an, dass nur der Netzwerkdatenverkehr, der von einem Mitglied des nag-Objekts stammt, zulässig ist.
- Die Server Isolierung kann auch unabhängig von einer isolierten Domäne konfiguriert werden. Konfigurieren Sie dazu nur die Geräte, die mit dem isolierten Server mit Verbindungssicherheitsregeln kommunizieren müssen, um die Authentifizierung zu implementieren und die nag-Mitgliedschaft zu überprüfen.
- Eine Server Isolations Zone kann gleichzeitig als Verschlüsselungszone konfiguriert werden. Konfigurieren Sie dazu das Gruppenrichtlinienobjekt mit Regeln, die die Verschlüsselung erzwingen, und die Authentifizierung und den Zugriff auf nag-Mitglieder einschränken. Weitere Informationen finden Sie unter anfordern von Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen.

Für dieses Bereitstellungsziel sind die folgenden Komponenten erforderlich:

- **Active Directory**: Active Directory unterstützt die zentralisierte Verwaltung von Verbindungssicherheitsregeln durch Konfigurieren der Regeln in einem oder mehreren GPOs, die automatisch auf alle relevanten Geräte in der Domäne angewendet werden können.

Nächster Schritt: Zuordnen Ihrer Bereitstellungsziele zu einer Windows Defender-Firewall mit erweitertem Sicherheits Design

Zuordnen Ihrer Bereitstellungsziele zu einem Entwurf für eine Windows-Firewall mit erweiterter Sicherheit

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie die Überprüfung der vorhandenen Windows-Firewall mit erweiterten Sicherheits Bereitstellungszielen abgeschlossen haben und feststellen, welche Ziele für Ihre spezifische Bereitstellung wichtig sind, können Sie diese Ziele einer bestimmten Windows-Firewall mit erweitertem Sicherheitsdesign zuordnen.

> **Wichtig:** die ersten drei in diesem Leitfaden vorgestellten Designs bauen auf einander auf, um von einfacher zu komplexer zu werden. Verwenden Sie daher während der Bereitstellung die Implementierung in der angegebenen Reihenfolge. Jedes bereitgestellte Design bietet auch eine stabile Position, von der Sie den Fortschritt bewerten und sicherstellen können, dass Ihre Ziele erfüllt werden, bevor Sie mit dem nächsten Entwurf fortfahren.

Ermitteln Sie anhand der folgenden Tabelle, welche Windows-Firewall mit erweitertem Sicherheitsdesign der entsprechenden Kombination der Windows-Firewall mit erweiterten Sicherheits Bereitstellungszielen für Ihre Organisation zugeordnet ist. Diese Tabelle bezieht sich nur auf die Windows-Firewall mit erweiterten Sicherheitsdesigns, wie in diesem Leitfaden beschrieben. Sie können jedoch eine Hybrid-oder benutzerdefinierte Windows-Firewall mit erweitertem Sicherheitsdesign erstellen, indem Sie eine beliebige Kombination der Windows-Firewall mit erweiterten Sicherheits Bereitstellungszielen verwenden, um die Anforderungen Ihrer Organisation zu erfüllen.

BEREITSTELLUNGSZIELE	ENTWURF EINER ALLGEMEINEN FIREWALLRICHTLINIE	ENTWURF EINER DOMÄNENISOLATIONS RICHTLINIE	ENTWURF EINER SERVERISOLATIONSRIC HTLINIE	ENTWURF EINER ZERTIFIKATBASIERTEN ISOLATIONSRICHTLINIE
Schützen von Geräten vor unerwünschtem Netzwerkverkehr	Ja	Ja	Ja	Ja
Beschränken des Zugriffs auf vertrauenswürdige Geräte	-	Ja	Ja	Ja
Einschränken des Zugriffs auf bestimmte Benutzer oder Geräte	-	-	Ja	Ja
Vorschreiben der Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen	-	Optional	Optional	Optional

Wenn Sie Details zu einem bestimmten Design untersuchen möchten, klicken Sie oben in der Spalte in der

vorhergehenden Tabelle auf den Design Titel.

Nächster Schritt: Grundlegender Firewall-Richtlinienentwurf

Entwurf einer allgemeinen Firewallrichtlinie

07.08.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Viele Organisationen verfügen über eine Netzwerkumkreis Firewall, die das Eindringen von böswilligem Datenverkehr in das Netzwerk der Organisation verhindern soll, auf jedem Gerät in der Organisation jedoch keine hostbasierte Firewall aktiviert ist.

Das grundlegende Design der Firewall-Richtlinie hilft Ihnen, die Geräte in Ihrer Organisation vor unerwünschtem Netzwerkdatenverkehr zu schützen, der durch die Verteidigung des Perimeters gelangt oder von Ihrem Netzwerk stammt. In diesem Entwurf stellen Sie Firewallregeln für jedes Gerät in Ihrer Organisation bereit, um Datenverkehr zuzulassen, der für die verwendeten Programme erforderlich ist. Datenverkehr, der den Regeln nicht entspricht, wird gelöscht.

Datenverkehr kann basierend auf den Merkmalen der einzelnen Netzwerkpakete blockiert oder zulässig sein: die Quell-oder Ziel-IP-Adresse, die Quell-oder Ziel-Portnummern, das Programm auf dem Gerät, das das eingehende Paket empfängt usw. Dieser Entwurf kann auch zusammen mit einem oder mehreren anderen Designs bereitgestellt werden, die dem zulässigen Netzwerkdatenverkehr IPSec-Schutz hinzufügen.

Viele Netzwerkadministratoren möchten nicht die schwierige Aufgabe angehen, alle geeigneten Regeln für jedes Programm zu ermitteln, das von der Organisation verwendet wird, und diese Liste dann im Laufe der Zeit beizubehalten. In der Tat sind für die meisten Programme keine bestimmten Firewallregeln erforderlich. Das Standardverhalten von Windows und den meisten zeitgenössischen Anwendungen macht diese Aufgabe einfach:

- Auf Clientgeräten unterstützt das Standardverhalten der Firewall bereits typische Clientprogramme. Programme erstellen alle erforderlichen Regeln für Sie im Rahmen des Installationsvorgangs. Sie müssen nur eine Regel erstellen, wenn das Clientprogramm in der Lage sein muss, unerwünschten eingehenden Netzwerkdatenverkehr von einem anderen Gerät zu empfangen.

- Wenn Sie ein Serverprogramm installieren, das unerwünschten eingehenden Netzwerkdatenverkehr akzeptieren muss, erstellt oder aktiviert das Installationsprogramm wahrscheinlich die entsprechenden Regeln auf dem Server für Sie.

  Wenn Sie beispielsweise eine Serverrolle installieren, werden die entsprechenden Firewallregeln automatisch erstellt und aktiviert.

- Bei anderen standardmäßigen Netzwerkverhalten können die vordefinierten Regeln, die in Windows Server 2012, Windows Server2008R2, Windows Server2008, Windows 8, Windows7 und Windows Vista integriert sind, problemlos in einem GPO konfiguriert und auf den Geräten in Ihrer Organisation bereitgestellt werden.

  Wenn Sie beispielsweise die vordefinierten Gruppen für das Kernnetzwerk und die Datei-und Druckerfreigabe verwenden, können Sie GPOs problemlos mit Regeln für die häufig verwendeten Netzwerkprotokolle konfigurieren.

Mit wenigen Ausnahmen kann die Firewall für alle Konfigurationen aktiviert werden. Wir empfehlen daher, die Firewall auf jedem Gerät in Ihrer Organisation zu aktivieren. Dazu gehören Server in Ihrem Umkreisnetzwerk, auf mobilen und Remoteclients, die eine Verbindung mit dem Netzwerk herstellen, sowie auf allen Servern und Clients in Ihrem internen Netzwerk.

> **Vorsicht:** das Beenden des Diensts, der mit der Windows Defender-Firewall mit erweiterter Sicherheit verbunden ist, wird von Microsoft nicht unterstützt.

Standardmäßig ist in neuen Installationen die Windows Defender-Firewall mit erweiterter Sicherheit in Windows Server 2012, Windows 8 und höher aktiviert.

Wenn Sie den Windows Defender-Firewalldienst deaktivieren, gehen andere Vorteile des Diensts verloren, beispielsweise die Möglichkeit, IPsec-Verbindungssicherheitsregeln, Windows-Diensthärtung und Netzwerkschutz vor Angriffsformen zu verwenden, die das Netzwerk verwenden. Fingerprinting.

Mit der kompatiblen Firewall-Software von Drittanbietern können nur die Teile der Windows Defender-Firewall programmgesteuert deaktiviert werden, die möglicherweise aus Kompatibilitätsgründen deaktiviert werden müssen. Dies ist die empfohlene Vorgehensweise für Firewalls von Drittanbietern, die mit der Windows Defender-Firewall koexistieren sollen. Firewalls von Drittanbietern, die dieser Empfehlung entsprechen, verfügen über das Certified-Logo von Microsoft.

Eine Organisation verwendet dieses Design in der Regel als ersten Schritt in Richtung eines umfassenderen Windows Defender-Firewall-Designs, das Serverisolierung und Domänenisolierung hinzufügt.

Nachdem Sie diesen Entwurf implementiert haben, verfügen Sie über eine zentralisierte Verwaltung der Firewallregeln, die auf alle Geräte angewendet werden, auf denen Windows in Ihrer Organisation ausgeführt wird.

> **Wichtig:** Wenn Sie auch den Entwurf der Domänen Isolierungs Richtlinieoder das Design der Server Isolierungs Richtlinie bereitstellen möchten, empfehlen wir, dass Sie die Entwurfsarbeit für alle drei Designs zusammen ausführen und dann in Ebenen bereitstellen, die dem entsprechen. mit jedem Design.

Das grundlegende Design der Firewall kann auf Geräte angewendet werden, die Teil einer Active Directory-Gesamtstruktur sind. Active Directory ist erforderlich, um die zentralisierte Verwaltung und Bereitstellung von Gruppenrichtlinienobjekten bereitzustellen, die die Firewalleinstellungen und-Regeln enthalten.

Weitere Informationen zu diesem Design:

- Dieser Entwurf fällt mit dem Bereitstellungsziel zusammen, um Geräte vor unerwünschtem Netzwerkdatenverkehr zu schützen.
- Weitere Informationen zu diesem Entwurf finden Sie unter Beispiel für Firewall-Richtlinienentwurf.
- Bevor Sie den Entwurf abschließen, sammeln Sie die Informationen, die unter Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategiebeschrieben sind.
- Informationen dazu, wie Sie die in diesem Entwurf erforderlichen Entscheidungen treffen können, finden Sie unter Planen von Einstellungen für eine grundlegende Firewall-Richtlinie.
- Eine Liste der detaillierten Aufgaben, die Sie für die Bereitstellung ihres grundlegenden Firewall-Richtlinien Designs verwenden können, finden Sie unter Checkliste: Implementieren eines grundlegenden Firewall-Richtlinienentwurfs.

Nächster Schritt: Entwurf einer Domänen Isolierungs Richtlinie

Entwurf einer Domänenisolationsrichtlinie

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

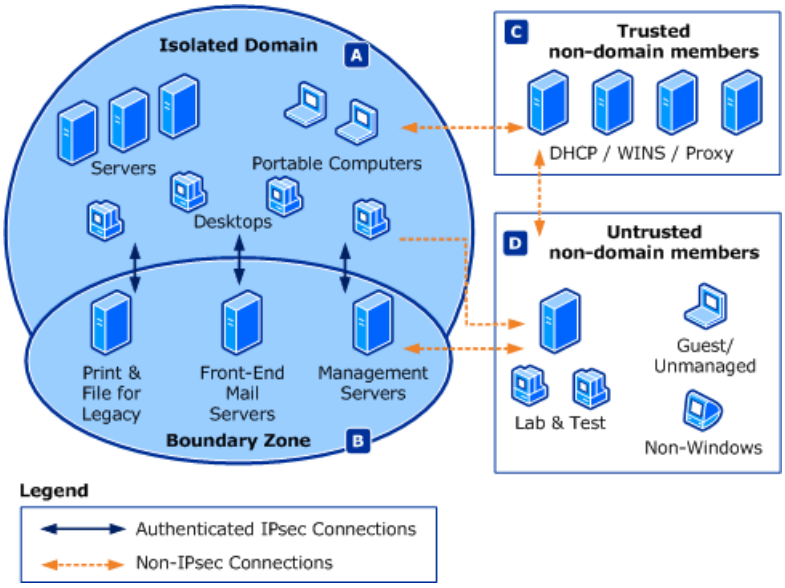
Im Entwurf der Domänen Isolierungs Richtlinie konfigurieren Sie die Geräte in Ihrem Netzwerk so, dass nur Verbindungen akzeptiert werden, die von Geräten stammen, die als Mitglieder derselben isolierten Domäne authentifiziert sind.

Dieser Entwurf beginnt in der Regel mit einem Netzwerk, das wie im Abschnitt Basic Firewall Policy Design beschrieben konfiguriert ist. Für diesen Entwurf fügen Sie dann Verbindungssicherheit und IPSec-Regeln hinzu, um Geräte in der isolierten Domäne so zu konfigurieren, dass nur Netzwerkdatenverkehr von anderen Geräten akzeptiert wird, die sich als Mitglied der isolierten Domäne authentifizieren können. Nach der Implementierung der neuen Regeln lehnen Ihre Geräte unerwünschten Netzwerkdatenverkehr von Geräten ab, die nicht Mitglieder der isolierten Domäne sind.

Bei der isolierten Domäne handelt es sich möglicherweise nicht um eine einzelne Active Directory-Domäne. Sie kann aus allen Domänen in einer Gesamtstruktur oder Domänen in getrennten Gesamtstrukturen bestehen, in denen zwischen Ihnen zweiseitige Vertrauensstellungen konfiguriert sind.

Mithilfe von Verbindungssicherheitsregeln, die auf IPSec basieren, stellen Sie eine logische Barriere zwischen Geräten bereit, selbst wenn Sie mit dem gleichen physikalischen Netzwerksegment verbunden sind.

Das Design wird in der folgenden Abbildung gezeigt, wobei die Pfeile die zulässigen Kommunikationspfade aufweisen.



Zu den Merkmalen dieses Entwurfs, wie in der Abbildung dargestellt, gehören die folgenden:

- Isolierte Domäne (Bereich a): Geräte in der isolierten Domäne erhalten unerwünschten eingehenden Datenverkehr nur von anderen Mitgliedern der isolierten Domäne oder von Geräten, auf die in Authentifizierungsausnahme Regeln verwiesen wird. Geräte in der isolierten Domäne können Datenverkehr an ein beliebiges Gerät senden. Dies umfasst nicht authentifizierten Datenverkehr zu Geräten, die sich nicht in der isolierten Domäne befinden. Geräte, die keiner Active Directory-Domäne

beitreten können, aber Zertifikate für die Authentifizierung verwenden können, können Teil der isolierten Domäne sein. Weitere Informationen finden Sie unter zertifikatbasiertes Isolierungs Richtlinien Design.

- Grenz Zone (Bereich B): Geräte in der Grenz Zone sind Teil der isolierten Domäne, können aber eingehende Verbindungen von nicht vertrauenswürdigen Geräten wie Clients im Internet akzeptieren.

  Geräte in der Grenzzonen Anforderung, erfordern aber keine Authentifizierung für die Kommunikation. Wenn ein Mitglied der isolierten Domäne mit einem Mitglied der Grenz Zone kommuniziert, wird der Datenverkehr authentifiziert. Wenn ein Gerät, das nicht Bestandteil der isolierten Domäne ist, mit einem Mitglied der Grenz Zone kommuniziert, wird der Datenverkehr nicht authentifiziert.

  Da Grenzzonen Geräte für den Netzwerkdatenverkehr von nicht vertrauenswürdigen und potenziell feindlichen Geräten verfügbar gemacht werden, müssen Sie sorgfältig verwaltet und gesichert werden. Setzen Sie nur die Geräte, auf die externe Geräte in dieser Zone zugreifen müssen. Verwenden Sie Firewallregeln, um sicherzustellen, dass der Netzwerkdatenverkehr nur für Dienste akzeptiert wird, die für nicht-Domänenmitglieds Geräte verfügbar gemacht werden sollen.

- Vertrauenswürdige nicht-Domänenmitglieder (Bereich C) – Geräte im Netzwerk, die keine Domänenmitglieder sind oder die IPSec-Authentifizierung nicht verwenden können, können durch Konfigurieren von Authentifizierungsausnahme Regeln kommunizieren. Mithilfe dieser Regeln können Geräte in der isolierten Domäne eingehende Verbindungen von diesen vertrauenswürdigen nicht-Domänenmitglieds Geräten akzeptieren.

- Nicht vertrauenswürdige nicht-Domänenmitglieder (Bereich D): Geräte, die nicht von Ihrer Organisation verwaltet werden und eine unbekannte Sicherheitskonfiguration aufweisen, müssen nur Zugriff auf die Geräte haben, die für Ihre Organisation erforderlich sind, um Ihre Geschäfte ordnungsgemäß durchzuführen. Die Domänenisolierung ist vorhanden, um eine logische Barriere zwischen diesen nicht vertrauenswürdigen Geräten und den Geräten Ihrer Organisation zu schaffen.

Nachdem Sie diesen Entwurf implementiert haben, verfügt Ihr Verwaltungsteam über eine zentralisierte Verwaltung der Firewall-und Verbindungssicherheitsregeln, die auf die Geräte in Ihrer Organisation angewendet werden.

> **Wichtig:** dieser Entwurf baut auf dem Standardentwurf für Firewall-Richtlinienauf und dient wiederum als Grundlage für das Design der Server Isolierungs Richtlinie. Wenn Sie alle drei bereitstellen möchten, empfiehlt es sich, die Entwurfsarbeit für alle drei zusammen zu erledigen und dann in der vorgestellten Reihenfolge bereitzustellen.

Dieser Entwurf kann auf Geräte angewendet werden, die Teil einer Active Directory-Gesamtstruktur sind. Active Directory ist erforderlich, um die zentralisierte Verwaltung und Bereitstellung von Gruppenrichtlinienobjekten bereitzustellen, die die Verbindungssicherheitsregeln enthalten.

Informationen zum Erweitern der isolierten Domäne, um Geräte einzubeziehen, die nicht Teil einer Active Directory-Domäne sein können, finden Sie unter zertifikatbasiertes Isolierungs Richtlinien Design.

Weitere Informationen zu diesem Design:

- Dieser Entwurf entspricht den Bereitstellungszielen, um Geräte vor unerwünschtem Netzwerkdatenverkehr zu schützen, den Zugriff auf vertrauenswürdige Geräte zu beschränkenund optional Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen zu erfordern.

- Weitere Informationen zu diesem Entwurf finden Sie im Beispiel zum Entwerfen von Domänen Isolierungs Richtlinien.

- Bevor Sie den Entwurf abschließen, sammeln Sie die Informationen, die unter Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategiebeschrieben sind.

- Informationen dazu, wie Sie die in diesem Entwurf erforderlichen Entscheidungen treffen können, finden Sie unter Planen von Domänen Isolierungs Zonen und Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen.
- Eine Liste der Aufgaben, die Sie für die Bereitstellung Ihres Domänen Isolierungs Richtlinien Designs verwenden können, finden Sie unter Checkliste: Implementieren eines Domänen Isolierungs Richtlinien Designs.

Nächster Schritt: Entwurf der Server Isolierungs Richtlinie

Entwurf einer Serverisolationsrichtlinie

07.08.2019 • 3 minutes to read

Betrifft

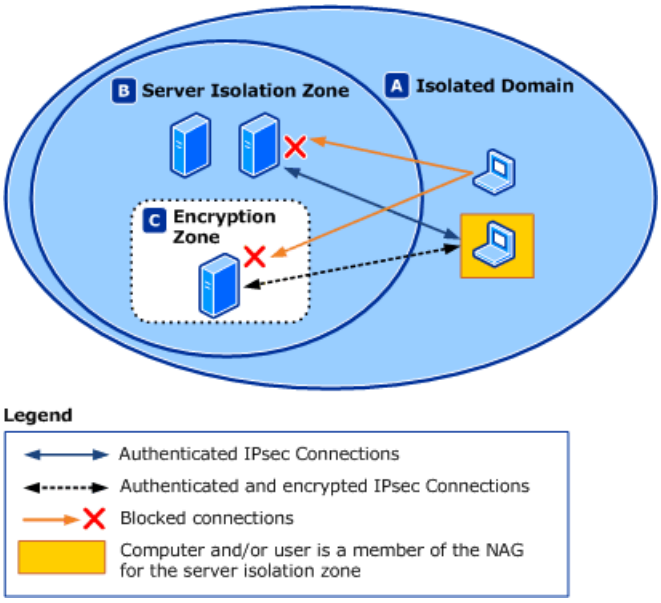
- Windows 10
- Windows Server 2016

Im Entwurf der Server Isolierungs Richtlinie weisen Sie einer Zone Server zu, die nur Zugriff auf Benutzer und Geräte gewährt, die sich als Mitglieder einer genehmigten Netzwerkzugriffsgruppe (NAG) authentifizieren.

Dieser Entwurf beginnt in der Regel mit einem Netzwerk, das wie im Abschnitt Entwerfen von Domänen Isolierungs Richtlinien beschrieben konfiguriert ist. Für dieses Design erstellen Sie Zonen für Server, die zusätzliche Sicherheitsanforderungen aufweisen. Die Zonen können den Zugriff auf den Server auf Mitglieder von autorisierten Gruppen beschränken und optional die Verschlüsselung des gesamten Datenverkehrs in oder aus diesen Servern anfordern. Dies kann auf pro-Server-Basis oder für eine Gruppe von Servern erfolgen, die gemeinsame Sicherheitsanforderungen aufweisen.

Sie können ein Server Isolierungs Design implementieren, ohne die Domänenisolierung zu verwenden. Dazu verwenden Sie die gleichen Prinzipien wie die Domänenisolierung, doch anstatt Sie auf eine Active Directory-Domäne anzuwenden, wenden Sie Sie nur auf die Geräte an, die auf die isolierten Server zugreifen können müssen. Das Gruppenrichtlinienobjekt enthält Verbindungssicherheit und Firewallregeln, die bei der Kommunikation mit den isolierten Servern eine Authentifizierung erfordern. In diesem Fall werden die Zugriffstasten, die ermitteln, welche Benutzer und Geräte auf den isolierten Server zugreifen können, auch verwendet, um zu ermitteln, welche Geräte das Gruppenrichtlinienobjekt empfangen.

Das Design wird in der folgenden Abbildung gezeigt, mit Pfeilen, die die zulässigen Kommunikationspfade anzeigen.



Zu den Merkmalen dieses Entwurfs gehören die folgenden:

- Isolierte Domäne (Bereich a) – dieselbe isolierte Domäne, die im Abschnitt Design für Domänen Isolierungs Richtlinien beschrieben wird. Wenn die isolierte Domäne eine Grenz Zone umfasst, Verhalten sich die Geräte in der Grenz Zone wie andere Mitglieder der isolierten Domäne so, wie Sie mit Geräten in Server Isolations Zonen interagieren.

- Isolierte Server (Bereich B): Geräte in den Server Isolations Zonen beschränken den Zugriff auf Geräte und optional auf Benutzer, die sich als Mitglied einer für den Zugriff autorisierten Netzwerkzugriffsgruppe (NAG) authentifizieren.
- Verschlüsselungszone (Bereich C): Wenn die Daten, die ausgetauscht werden, hinreichend sensibel sind, kann für die Verbindungssicherheitsregeln für die Zone auch die Verschlüsselung des Netzwerkverkehrs erforderlich sein. Verschlüsselungs Zonen werden am häufigsten als Regeln implementiert, die Teil einer Server Isolations Zone sind, anstatt als separate Zone. Das Diagramm veranschaulicht das Konzept als Teilmenge nur für konzeptuelle Zwecke.

Wenn Sie Unterstützung für die Serverisolierung hinzufügen möchten, müssen Sie sicherstellen, dass die Authentifizierungsmethoden mit den Anforderungen des isolierten Servers kompatibel sind. Wenn Sie beispielsweise Benutzerkonten, die Mitglieder eines nag sind, zusätzlich zur Autorisierung von Computerkonten autorisieren möchten, müssen Sie sowohl die Benutzer-als auch die Computerauthentifizierung in ihren Verbindungssicherheitsregeln aktivieren.

> **Wichtig:** dieser Entwurf baut auf dem Design der Domänen Isolierungs Richtlinieauf, das wiederum auf dem grundlegenden Design der Firewall-Richtlinienbasiert. Wenn Sie alle drei Entwürfe bereitstellen möchten, führen Sie den Entwurf für alle drei zusammen aus, und stellen Sie dann in der vorgestellten Reihenfolge bereit.

Dieser Entwurf kann auf Geräte angewendet werden, die Teil einer Active Directory-Gesamtstruktur sind. Active Directory ist erforderlich, um die zentralisierte Verwaltung und Bereitstellung von Gruppenrichtlinienobjekten bereitzustellen, die die Verbindungssicherheitsregeln enthalten.

Weitere Informationen zu diesem Design:

- Dieser Entwurf fällt mit den Bereitstellungszielen zusammen, um Geräte vor unerwünschtem Netzwerkdatenverkehr zu schützen, den Zugriff auf vertrauenswürdige Geräte zu beschränken, den Zugriff auf bestimmte Benutzer oder Geräte zu beschränkenund die Verschlüsselung zu erfordern, Wenn Zugriff auf vertrauliche Netzwerkressourcen.
- Weitere Informationen zu diesem Entwurf finden Sie unter Beispiel für den Entwurf der Server Isolierungs Richtlinie.
- Bevor Sie den Entwurf abschließen, sammeln Sie die Informationen, die unter Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategiebeschrieben sind.
- Informationen dazu, wie Sie die in diesem Entwurf erforderlichen Entscheidungen treffen können, finden Sie unter Planen von Server Isolations Zonen und Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen.
- Eine Liste der Aufgaben, die Sie für die Bereitstellung Ihres Server Isolations Richtlinien Designs verwenden können, finden Sie unter Checkliste: Implementieren eines eigenständigen Richtlinienentwurfs für die Serverisolierung.

Nächster Schritt: Entwurf einer zertifikatbasierten Isolierungs Richtlinie

Entwurf einer zertifikatbasierten Isolationsrichtlinie

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Beim Entwurf der zertifikatbasierten Isolierungs Richtlinie stellen Sie die gleichen Schutztypen für den Netzwerkdatenverkehr bereit wie in den Abschnitten " Domänen Isolierungs Richtlinienentwurf " und " Server Isolierungs Richtlinienentwurf" beschrieben. Der einzige Unterschied ist die Methode, mit der Identifikations Anmeldeinformationen während der Authentifizierung Ihres Netzwerkdatenverkehrs freigegeben werden.

Domänenisolierung und Serverisolierung bieten Sicherheit für die Geräte im Netzwerk, die Windows ausführen und mit einer Active Directory-Domäne verbunden werden können. In den meisten Unternehmensumgebungen sind jedoch in der Regel einige Geräte vorhanden, die ein anderes Betriebssystem ausführen müssen. Diese Geräte können nicht an einer Active Directory-Domäne teilnehmen, ohne dass ein Drittanbieter Paket installiert wird. Außerdem können einige Geräte, auf denen Windows ausgeführt wird, aus unterschiedlichen Gründen nicht an einer Domäne teilnehmen. Wenn Sie Kerberos V5 als Authentifizierungsprotokoll verwenden möchten, muss das Gerät mit dem Active Directory verbunden sein und (für nicht-Windows-Geräte) Kerberos als Authentifizierungsprotokoll unterstützen.

Zur Authentifizierung mit nicht-Domänenmitglieds Geräten unterstützt IPSec die Verwendung standardbasierter kryptografischer Zertifikate. Da diese Authentifizierungsmethode auch von vielen Betriebssystemen von Drittanbietern unterstützt wird, kann Sie als Möglichkeit zum Erweitern Ihrer isolierten Domäne auf Geräte verwendet werden, die Windows nicht ausführen.

Für diesen Entwurf gelten die gleichen Prinzipien wie für die Domänen-und Server Isolierungs Designs. Nur Geräte, die sich authentifizieren können (in diesem Fall durch Bereitstellen eines angegebenen Zertifikats), können mit den Geräten in ihrer isolierten Domäne kommunizieren.

Für Windows-Geräte, die Teil einer Active Directory-Domäne sind, können Sie mithilfe von Gruppenrichtlinien die Zertifikate bereitstellen, die für die Kommunikation mit den vertrauenswürdigen Geräten erforderlich sind, aber nicht Teil der Active Directory-Domäne sind. Bei anderen Geräten müssen Sie diese entweder manuell mit den erforderlichen Zertifikaten konfigurieren oder ein Programm eines Drittanbieters verwenden, um die Zertifikate auf sichere Weise zu verteilen.

Weitere Informationen zu diesem Design:

- Dieser Entwurf entspricht den Bereitstellungszielen, um Geräte vor unerwünschtem Netzwerkdatenverkehr zu schützen, den Zugriff auf vertrauenswürdige Geräte zu beschränkenund optional Verschlüsselung beim Zugriff auf vertrauliche Netzwerkressourcen zu erfordern.
- Weitere Informationen zu diesem Entwurf finden Sie unter zertifikatbasierte Isolierungs Richtlinien-Entwurfsbeispiel.
- Bevor Sie den Entwurf abschließen, sammeln Sie die Informationen, die unter Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategiebeschrieben sind.
- Informationen dazu, wie Sie die in diesem Entwurf erforderlichen Entscheidungen treffen können, finden Sie unter Planen der zertifikatbasierten Authentifizierung.
- Eine Liste der Aufgaben, die Sie zum Bereitstellen des zertifikatsbasierten Richtlinienentwurfs verwenden

können, finden Sie unter Checkliste: Implementieren eines zertifikatsbasierten Isolierungs Richtlinien Designs.

Nächster Schritt: Auswerten der Windows Defender-Firewall mit erweiterten Sicherheitsentwurfs Beispielen

Auswerten der Windows Defender-Firewall mit erweiterten Sicherheitsentwurfs Beispielen

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die folgende Windows Defender-Firewall mit erweiterten Sicherheitsdesign-Beispielen veranschaulichen, wie Sie die Windows Defender-Firewall verwenden können, um die Sicherheit der an das Netzwerk angeschlossenen Geräte zu verbessern. Mithilfe dieser Themen können Sie auswerten, wie die Firewall-und Verbindungssicherheitsregeln für alle Windows Defender-Firewall-Designs funktionieren, und ermitteln, welche Designs oder Kombinationen von Entwürfen für die Ziele Ihrer Organisation am besten geeignet sind.

- Firewall-Richtlinie mit erweitertem Sicherheits Design (Beispiel)
- Beispiel für den Entwurf einer Domänenisolationsrichtlinie
- Beispiel für den Entwurf einer Serverisolationsrichtlinie
- Beispiel für den Entwurf einer zertifikatbasierten Isolationsrichtlinie

Beispiel für den Entwurf einer Firewallrichtlinie

07.08.2019 • 7 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Beispiel ist das fiktive Unternehmen Woodgrove Bank eine Finanz Dienstleistungseinrichtung.

Die Woodgrove Bank verfügt über eine Active Directory-Domäne, die gruppenrichtlinienbasierte Verwaltung für alle Windows-Geräte bereitstellt. Die Active Directory-Domänencontroller hosten auch DNS (Domain Name System) für die Hostnamensauflösung. Separate Geräte hosten den Windows Internet Name Service (WINS) für die NetBIOS-Namensauflösung (Network Basic Input/Output System). Bei einer Reihe von Geräten, auf denen UNIX ausgeführt wird, stehen die DHCP-Dienste (Dynamic Host Configuration Protocol) für die automatische IP-Adressierung zur Verfügung.

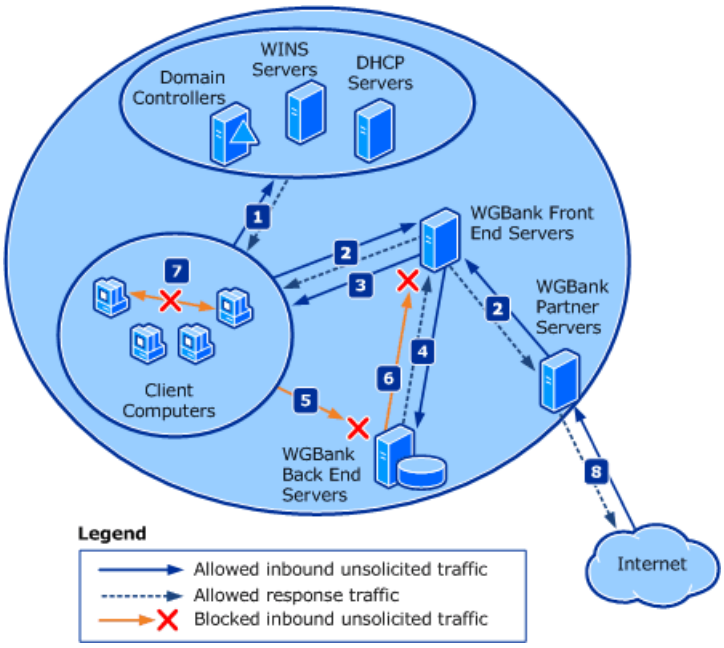
Die Woodgrove Bank ist dabei, Ihre Geräte von Windows Vista und Windows Server2008 auf Windows 10 und Windows Server 2016 zu migrieren. Eine beträchtliche Anzahl von Geräten der Woodgrove Bank führt weiterhin Windows Vista und Windows Server2008 aus. Die Interoperabilität zwischen dem vorherigen und neueren Betriebssystemen muss beibehalten werden. Wenn möglich, müssen die Sicherheitsfeatures, die auf neuere Betriebssysteme angewendet werden, auch auf die vorherigen Betriebssysteme angewendet werden.

Ein wichtiges Branchen Programm namens WGBank besteht aus einem Clientprogramm, das auf den meisten Desktopgeräten in der Organisation ausgeführt wird. Dieses Programm greift auf mehrere Front-End-Server Geräte zu, die den serverseitigen Teil von WGBank ausführen. Bei diesen Front-End-Servern wird nur die Verarbeitung durchführen – die Daten werden nicht gespeichert. Die Daten werden in mehreren Back-End-Daten Bank Geräten gespeichert, auf denen Microsoft SQL Server ausgeführt wird.

Entwurfsanforderungen

Die Netzwerkadministratoren möchten die Windows Defender-Firewall mit erweiterter Sicherheit in ihrer gesamten Organisation implementieren, um eine zusätzliche Sicherheitsschicht für Ihre allgemeine Sicherheitsstrategie bereitzustellen. Sie möchten Firewallregeln erstellen, die es ermöglichen, dass Ihre Geschäftsprogramme funktionieren, während der nicht gewünschte Netzwerkdatenverkehr blockiert wird.

Die folgende Abbildung zeigt den Datenschutz Bedarf für dieses Entwurfsbeispiel.



1. Die Netzwerkinfrastrukturserver, auf denen Dienste ausgeführt werden, wie Active Directory, DNS, DHCP oder WINS, können unaufgefordert eingehende Anforderungen von Netzwerkclients empfangen. Die Netzwerkclients können die Antworten von den Infrastrukturservern empfangen.
2. Die WGBank-Front-End-Server können unerwünschten eingehenden Datenverkehr von den Clientgeräten und den WGBank-Partnerservern empfangen. Die WGBank-Clientgeräte und-Partnerserver können die Antwort empfangen.
3. Die WGBank-Front-End-Server können aktualisierte Informationen an die Clientgeräte senden, um die Echtzeitanzeige zu unterstützen. Die Clients können diesen unerbetenen Datenverkehr nicht Abfragen, müssen ihn aber empfangen können.
4. Die WGBank-Back-End-Server können SQL-Abfrageanforderungen von den WGBank-Front-End-Servern empfangen. Die WGBank-Front-End-Server können die entsprechenden Antworten empfangen.
5. Es gibt keine direkte Kommunikation zwischen den Clientgeräten und den WGBank-Back-End-Geräten.
6. Von den WGBank-Back-End-Geräten an die WGBank-Front-End-Server gibt es keinen unerbetenen Datenverkehr.
7. Unternehmensrichtlinien verbietet die Verwendung von Peer-to-Peer-Dateiübertragungssoftware. Eine kürzlich durchgeführte Überprüfung der IT-Mitarbeiter hat festgestellt, dass die Umkreisfirewall zwar verhindert, dass die meisten Programme in dieser Kategorie funktionieren, aber zwei Programme von Mitarbeitern verwendet werden, für die kein externer Server erforderlich ist. Firewallregeln müssen den von diesen Programmen erstellten Netzwerkdatenverkehr blockieren.
8. Die WGBank-Partnerserver können eingehende Anfragen von Partner Geräten über das Internet empfangen.

Andere Verkehrshinweise:

- Geräte dürfen keinen unerwünschten Datenverkehr von einem anderen als den oben genannten Computer empfangen.
- Anderer Ausgeh ender Netzwerkdatenverkehr von den Clientgeräten, die in diesem Beispiel nicht ausdrücklich identifiziert werden, ist zulässig.

Entwurfsdetails

Die Woodgrove Bank verwendet Active Directory-Gruppen und Gruppenrichtlinienobjekte, um die

Firewalleinstellungen und-Regeln für die Geräte in Ihrem Netzwerk bereitzustellen. Sie wissen, dass Sie Richtlinien für die folgenden gerätesammlungen bereitstellen müssen:

- Client Geräte, die Windows 10, Windows 8 oder Windows7 ausführen
- WGBank-Front-End-Server, auf denen Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 oder Windows Server2008R2 ausgeführt wird (noch keine vorhanden, aber Ihre Lösung muss das Hinzufügen unterstützen)
- WGBank-Partnerserver, auf denen Windows Server2008 ausgeführt wird
- WGBank-Back-End-SQL Server-Geräte, auf denen Windows Server2008 ausgeführt wird (es sind noch keine vorhanden, aber Ihre Lösung muss das Hinzufügen unterstützen)
- Infrastrukturserver, auf denen Windows Server2008 ausgeführt wird
- Active Directory-Domänencontroller, die Windows Server2008R2 oder Windows Server 2012 ausführen
- DHCP-Server, auf denen das UNIX-Betriebssystem ausgeführt wird

Nachdem Sie diese Gerätegruppen ausgewertet und mit der Struktur der Active Directory-Organisationseinheit (OU) verglichen haben, haben die Netzwerkadministratoren der Woodgrove Bank festgestellt, dass es keine gute 1:1-Übereinstimmung zwischen den OUs und den Gruppen gibt. Daher werden die Firewall-GPOs nicht direkt mit OUs verknüpft, in denen die relevanten Geräte enthalten sind. Stattdessen sind die GPOs mit dem Domänencontainer in Active Directory verknüpft, und dann werden WMI-und Gruppenfilter an das Gruppenrichtlinienobjekt angefügt, um sicherzustellen, dass es auf die richtigen Geräte angewendet wird.

Durch das Einrichten von Gruppen, wie hier beschrieben, wird sichergestellt, dass Sie nicht wissen müssen, welches Betriebssystem ein Computer ausführt, bevor Sie es einer Gruppe zuweisen. Eine Kombination aus WMI-Filtern und Sicherheitsgruppen Filtern wird verwendet, um sicherzustellen, dass die Mitglieder der Gruppe das Gruppenrichtlinienobjekt erhalten, das für die auf diesem Computer ausgeführte Windows-Version geeignet ist. Für einige Gruppen verfügen Sie möglicherweise über vier oder sogar fünf GPOs.

Die folgenden Gruppen wurden mithilfe des MMC-Snap-Ins (Microsoft Management Console) Active Directory-Benutzer und-Computer erstellt, und alle Geräte, auf denen Windows ausgeführt wurde, wurden den richtigen Gruppen hinzugefügt:

- **CG_FIREWALL_ALLCOMPUTERS**. Fügen Sie die vordefinierte und System verwaltete **Domäne "Computer** " als Mitglied dieser Gruppe hinzu. Alle Mitglieder der FIREWALL_ALLCOMPUTERS-Gruppe erhalten ein Betriebssystem spezifisches GPO mit den allgemeinen Firewallregeln, die auf alle Geräte angewendet werden.

  Die beiden Gerätetypen (Client und Server) werden mithilfe einer WMI-Filter unterschieden, um sicherzustellen, dass nur die Richtlinie für Geräte, die eine Client Version von Windows ausführen, auf diesen Computer angewendet werden kann. Ein ähnlicher WMI-Filter für das Server-Gruppenrichtlinienobjekt stellt sicher, dass nur Geräte, auf denen Server Versionen von Windows ausgeführt werden, das Gruppenrichtlinienobjekt anwenden können. Jedes der GPOs verfügt auch über Sicherheitsgruppenfilter, um zu verhindern, dass Mitglieder der Gruppe FIREWALL_NO_DEFAULT eine dieser beiden GPOs empfangen.

  - Client Geräte erhalten ein GPO, das die Windows Defender-Firewall so konfiguriert, dass das Standardverhalten der Windows Defender-Firewall erzwungen wird (ausgehendes zulassen, unerwünschtes eingehen blockieren). Das standardmäßige Client-GPO umfasst auch die integrierten Firewall-Regelgruppen Kernnetzwerk und Datei-und Druckerfreigabe. Die zentrale Netzwerkgruppe ist für alle Profile aktiviert, während die Datei-und Druckerfreigabe Gruppe nur für die Domänen-und privaten Profile aktiviert ist. Das Gruppenrichtlinienobjekt enthält auch eingehende Firewallregeln, um dem WGBank-Front-End-Server-Dashboard-Update Datenverkehr zu ermöglichen, und Regeln, um zu verhindern, dass vom Unternehmen Verbotene Programme

Netzwerkdatenverkehr sowohl eingehend als auch ausgehende senden oder empfangen.

    - Server Geräte erhalten ein GPO, das eine ähnliche Firewall-Konfiguration für das GPO des Clientcomputers umfasst. Der Hauptunterschied besteht darin, dass die Regeln für alle Profile aktiviert sind (nicht nur für Domäne und privat). Darüber hinaus sind die Regeln für das WGBank-Dashboard-Update nicht enthalten, da es auf Server Geräten nicht erforderlich ist.

  Alle Regeln sind für den Bereich vorgesehen, um Netzwerkdatenverkehr nur von Geräten im Unternehmensnetzwerk der Woodgrove Bank zu ermöglichen.

- **CG_FIREWALL_NO_DEFAULT**. Mitglieder dieser Gruppe erhalten nicht das standardmäßige Firewall-Gruppenrichtlinienobjekt. Geräte werden dieser Gruppe hinzugefügt, wenn es eine geschäftliche Anforderung gibt, dass Sie vom Standardverhalten der Firewall ausgenommen werden kann. Die Verwendung einer Gruppe, um die Ausnahmen anstelle der Gruppenmitglieder direkt darzustellen, erleichtert die Unterstützung des dynamischen Charakters der Clientcomputer Population. Ein neuer Computer, der der Domäne beigetreten ist, erhält automatisch das entsprechende standardmäßige Firewall-GPO, es sei denn, es handelt sich um ein Mitglied dieser Gruppe.

- **CG_FIREWALL_WGB_FE**. Diese Gruppe enthält die Computerkonten für alle WGBank-Front-End-Server Geräte. Mitglieder dieser Gruppe erhalten ein GPO, das die Windows Defender-Firewall mit eingehenden Firewallregeln so konfiguriert, dass unerwünschter WGBank-Client Datenverkehr zulässig ist. Geräte in dieser Gruppe erhalten auch das standardmäßige Firewall-Gruppenrichtlinienobjekt.

- **CG_FIREWALL_WGB_SQL**. Diese Gruppe enthält die Computerkonten für alle WGBank-Back-End-Geräte, auf denen SQL Server ausgeführt wird. Mitglieder dieser Gruppe erhalten ein GPO, das die Windows Defender-Firewall mit eingehenden Firewall-Regeln konfiguriert, damit das SQL Server-Programm unerwünschte Abfragen nur von den WGBank-Front-End-Servern empfangen kann. Geräte in dieser Gruppe erhalten auch das standardmäßige Firewall-Gruppenrichtlinienobjekt.

- **CG_FIREWALL_BOUNDARY_WGBANKFE**. Diese Gruppe enthält die Computerkonten für die Server, auf denen Webdienste gehostet werden, auf die über das Internet zugegriffen werden kann. Mitglieder dieser Gruppe erhalten ein GPO, das eine eingehende Firewallregel hinzufügt, um eingehenden HTTP-und HTTPS-Netzwerkdatenverkehr von beliebigen Adressen, einschließlich des Internets, zuzulassen. Geräte in dieser Gruppe erhalten auch das standardmäßige Firewall-Gruppenrichtlinienobjekt.

- **CG_FIREWALL_WINS**. Diese Gruppe enthält die Computerkonten für alle WINS-Server Geräte. Mitglieder dieser Gruppe erhalten ein GPO, das die Windows Defender-Firewall mit einer eingehenden Firewall-Regel konfiguriert, um nicht angeforderte eingehende Anfragen von WINS-Clients zu ermöglichen. Geräte in dieser Gruppe erhalten auch das standardmäßige Firewall-Gruppenrichtlinienobjekt.

- **CG_FIREWALL_ADDC**. Diese Gruppe enthält alle Computerkonten für die Active Directory-Domänencontroller-Server Geräte. Mitglieder dieser Gruppe erhalten ein GPO, das die Windows Defender-Firewall mit eingehenden Firewall-Regeln konfiguriert, um unerwünschten Active Directory-Client-und Server-zu-Server-Datenverkehr zu ermöglichen. Geräte in dieser Gruppe erhalten auch das standardmäßige Firewall-Gruppenrichtlinienobjekt.

Erstellen Sie in Ihrem eigenen Entwurf eine Gruppe für jede Computerrolle in Ihrer Organisation, die unterschiedliche oder zusätzliche Firewallregeln erfordert. Beispielsweise erfordern Dateiserver und Druckserver zusätzliche Regeln, damit der eingehende Netzwerkdatenverkehr für diese Funktionen zugelassen wird. Wenn eine Funktion normalerweise auf den meisten Geräten im Netzwerk ausgeführt wird, sollten Sie das Hinzufügen von Geräten, die diese Rollen ausführen, zum gemeinsamen standardmäßigen Gruppenrichtlinien-Gruppenrichtlinienobjekt hinzufügen, es sei denn, es gibt einen Sicherheitsgrund, ihn nicht dort einzuschließen.

Nächster Schritt: Design Beispiel für Domänen Isolierungs Richtlinien

Beispiel für den Entwurf einer Domänenisolationsrichtlinie

07.08.2019 • 4 minutes to read

Betrifft

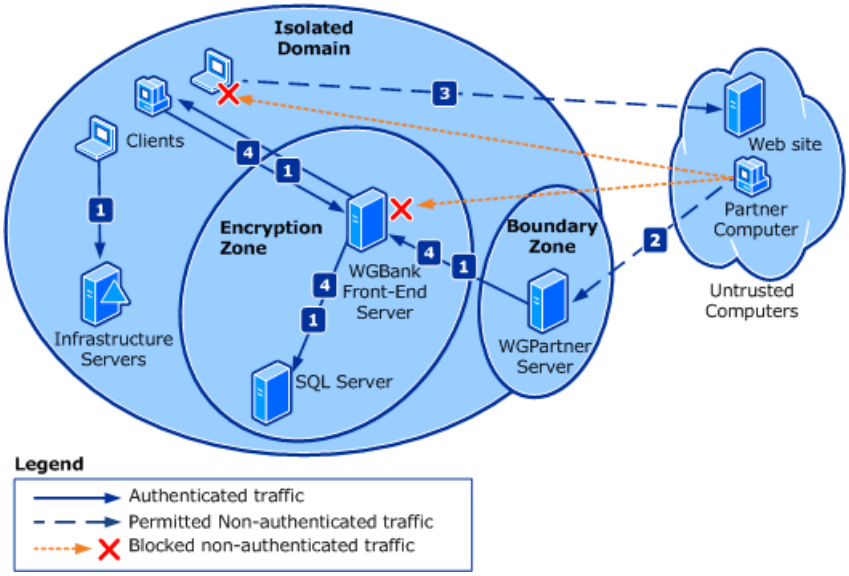
- Windows 10
- Windows Server 2016

Dieses Entwurfsbeispiel verwendet weiterhin das fiktive Unternehmen Woodgrove Bank und baut auf dem Beispiel, das im Abschnitt Firewall-Richtlinien Design beschrieben wird. In diesem Beispiel finden Sie eine Erläuterung der grundlegenden Unternehmensnetzwerk Infrastruktur bei der Woodgrove Bank mit Diagrammen.

Entwurfsanforderungen

Neben dem Standardschutz, der durch die Firewallregeln im vorherigen Entwurfsbeispiel bereitgestellt wird, möchten Sie möglicherweise die Domänenisolierung implementieren, um ihren verteilten Geräten eine weitere Sicherheitsebene bereitzustellen. Sie können Firewall-und Verbindungssicherheitsregeln erstellen, die die Authentifizierung verwenden, um das Risiko der Kommunikation mit nicht vertrauenswürdigen und potenziell feindlichen Geräten zu verringern.

Die folgende Abbildung zeigt den Datenschutz, der für dieses Entwurfsbeispiel erforderlich ist.



1. Alle Geräte im Unternehmensnetzwerk der Woodgrove Bank, die Active Directory-Domänenmitglieder sind, müssen eingehenden Netzwerkdatenverkehr authentifizieren, wenn Sie von einem anderen Computer stammen, der Mitglied der Domäne ist. Sofern in diesem Abschnitt nicht anders angegeben, lehnen die Woodgrove Bank-Geräte alle nicht angeforderten eingehenden Netzwerkdatenverkehr ab, die nicht authentifiziert sind. Wenn das grundlegende Firewall-Design ebenfalls implementiert ist, wird auch der authentifizierte eingehende Netzwerkdatenverkehr gelöscht, es sei denn, er entspricht einer eingehenden Firewall-Regel.

2. Die Server, die die WGPartner-Programme hosten, müssen in der Lage sein, unerwünschten eingehenden Datenverkehr von Geräten zu empfangen, die ihren Partnern gehören, die keine Mitglieder der Woodgrove Bank-Domäne sind.

3. Client Geräte können nicht authentifizierte ausgehende Kommunikationen mit Geräten initiieren, die keine Mitglieder der Domäne sind, beispielsweisedurch suchen externer Websites. Unerbetener eingehender Datenverkehr von nicht-Domänenmitgliedern wird blockiert.

4. Geräte im Verschlüsselungsbereich erfordern, dass der gesamte eingehende und ausgehende Netzwerkdatenverkehr verschlüsselt werden muss, zusätzlich zu der Authentifizierung, die für die isolierte Domäne bereits erforderlich ist.

Andere Verkehrshinweise:

- Alle im Abschnitt " Firewall-Richtlinienentwurf " beschriebenen Entwurfsanforderungen werden weiterhin erzwungen.

Entwurfs Details

Die Woodgrove Bank verwendet Active Directory-Gruppen und-GPOs, um die Domänen Isolationseinstellungen und-Regeln für die Geräte im Netzwerk bereitzustellen.

Durch das Einrichten von Gruppen, wie hier beschrieben, wird sichergestellt, dass Sie nicht wissen müssen, welches Betriebssystem ein Computer ausführt, bevor Sie es einer Gruppe zuweisen. Wie beim Entwurf der Firewall-Richtlinie wird eine Kombination aus WMI-Filtern und Sicherheitsgruppen Filtern verwendet, um sicherzustellen, dass die Mitglieder der Gruppe das Gruppenrichtlinienobjekt erhalten, das für die auf diesem Computer ausgeführte Version von Windows geeignet ist. Für einige Gruppen verfügen Sie möglicherweise über vier oder sogar fünf GPOs.

Die folgenden Gruppen wurden mit dem MMC-Snap-in Active Directory-Benutzer und-Computer erstellt, alle Geräte, auf denen Windows ausgeführt wurde, wurden den richtigen Gruppen hinzugefügt, und dann wird das entsprechende Gruppenrichtlinienobjekt auf die Gruppe angewendet. Wenn Sie ein Gerät in die isolierte Domäne oder eine der untergeordneten Zonen einbeziehen möchten, fügen Sie einfach das Konto des Geräts in der entsprechenden Gruppe hinzu.

- **CG_DOMISO_ISOLATEDDOMAIN**. Die Mitglieder dieser Gruppe sind an der isolierten Domäne beteiligt. Nach einem anfänglichen Pilot Zeitraum, gefolgt von einer langsam steigenden Gruppenmitgliedschaft, wurde die Mitgliedschaft dieser Gruppe schließlich durch die Eintrags **Domänencomputer** ersetzt, um sicherzustellen, dass alle Geräte in der Domäne standardmäßig teilnehmen. Die WMI-Filter stellen sicher, dass das Gruppenrichtlinienobjekt nicht auf Domänencontroller angewendet wird. GPOs mit Verbindungssicherheitsregeln zum Erzwingen des Domänen Isolations Verhaltens sind mit dem Domänencontainer verknüpft und auf die Geräte in dieser Gruppe angewendet. Filter stellen sicher, dass jeder Computer das richtige Gruppenrichtlinienobjekt für seinen Betriebssystemtyp erhält. Die Regeln im Gruppenrichtlinienobjekt für die Domänenisolierung erfordern die KerberosV5-Authentifizierung für eingehende Netzwerkverbindungen, und Sie können Sie für alle ausgehenden Verbindungen anfordern (aber nicht erforderlich).

- **CG_DOMISO_NO_IPSEC**. Dieser Gruppe werden die Berechtigungen Lesen oder Anwenden für alle Domänen Isolierungs Richtlinienobjekte verweigert. Dieser Gruppe werden alle Computer hinzugefügt, die nicht an der Domänenisolierung teilnehmen können, beispielsweise ein DHCP-Server, auf dem UNIX ausgeführt wird.

- **CG_DOMISO_BOUNDARY**. Diese Gruppe enthält die Computerkonten für alle Geräte, die Teil der Grenzgruppe sind und unangeforderten eingehenden Datenverkehr von nicht vertrauenswürdigen Geräten empfangen können. Mitglieder der Gruppe erhalten ein GPO, das die Verbindungssicherheitsregeln so konfiguriert, dass die eingehende und ausgehende Authentifizierung angefordert (aber nicht erforderlich) wird.

- **CG_DOMISO_ENCRYPTION**. Diese Gruppe enthält die Computerkonten für alle Geräte, für die ein-und ausgehenden Datenverkehr sowohl authentifiziert als auch verschlüsselt werden müssen. Mitglieder der

Gruppe erhalten ein GPO, das die Verbindungssicherheit und Firewallregeln so konfiguriert, dass für alle eingehenden und ausgehenden Datenverkehr sowohl Authentifizierung als auch Verschlüsselung erforderlich ist.

Hinweis: Wenn Sie GPOs nur für Windows 8, Windows7, Windows Vista, Windows Server 2012, Windows Server2008 und Windows Server2008R2 entwerfen, können Sie Ihre GPOs in geschachtelten Gruppen entwerfen. So können Sie beispielsweise die umgrenzungs Gruppe zu einem Mitglied der Gruppe der isolierten Domänen machen, sodass Sie die Firewall und die grundlegenden Einstellungen für die isolierte Domäne über diese geschachtelte Mitgliedschaft erhält, wobei nur die Änderungen durch das Gruppenrichtlinienobjekt für Grenzzonen bereitgestellt werden. Geräte, auf denen ältere Windows-Versionen ausgeführt werden, können jedoch nur eine einzelne IPSec-Richtlinie unterstützen, die gleichzeitig aktiv ist. Die Richtlinien für die einzelnen Gruppenrichtlinienobjekte müssen vollständig (und in hohem Maße redundant miteinander) sein, da Sie Sie in den neueren Versionen von Windows nicht wie möglich überlagern können. Aus Gründen der Einfachheit werden in diesem Leitfaden die Techniken beschrieben, mit denen unabhängige, nicht mehrschichtige Richtlinien erstellt werden. Wir empfehlen, dass Sie ein Skript erstellen und in regelmäßigen Abständen ausführen, das die Mitgliedschaften der Gruppen vergleicht, die sich gegenseitig ausschließen müssen, und Berichte über alle Geräte, die fälschlicherweise mehr als einer Gruppe zugeordnet sind.

Nächster Schritt: Design Beispiel für Server Isolierungs Richtlinien

Beispiel für den Entwurf einer Serverisolationsrichtlinie

07.08.2019 • 5 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Entwurfsbeispiel wird weiterhin das fiktive Unternehmen Woodgrove Bank verwendet, wie im Abschnitt Firewall-Richtlinien Design und im Beispielabschnitt zum Entwerfen von Domänen Isolierungs Richtlinien beschrieben.

Zusätzlich zu den Schutzbestimmungen, die von der Firewall und der Domänenisolierung bereitgestellt werden, möchte die Woodgrove Bank zusätzlichen Schutz für die Geräte bereitstellen, auf denen Microsoft SQL Server für das WGBank-Programm ausgeführt wird. Sie enthalten personenbezogene Daten, einschließlich der Finanzhistorie des Kunden. Richtlinien und Richtlinien für Behörden und Branchen geben an, dass der Zugriff auf diese Informationen nur auf die Benutzer beschränkt werden muss, die eine legitime geschäftliche Anforderung haben. Dies umfasst eine Anforderung, um das Abfangen von und den Zugriff auf die Informationen zu verhindern, wenn Sie über das Netzwerk übertragen werden.

Die Informationen, die von den WGBank-Front-End-Servern an die Clientgeräte übermittelt werden, und die Informationen, die die WGPartner-Server den Remote-Partner Geräten zur Verfügung gestellt haben, werden für die Zwecke der behördlichen Regelungen nicht als sensibel eingestuft, da Sie wird verarbeitet, um vertrauliche Elemente zu entfernen, bevor die Daten an die Clientgeräte übertragen werden.

In diesem Leitfaden werden in den Beispielen die Serverisolation auf einem Domänen Isolierungs Entwurf überlagert. Wenn Sie über eine isolierte Domäne verfügen, sind die Clientgeräte bereits mit GPOs ausgestattet, die eine Authentifizierung erfordern. Sie müssen nur den isolierten Servern Einstellungen hinzufügen, um eine Authentifizierung für eingehende Verbindungen zu erzwingen und die Mitgliedschaft im Nag zu überprüfen. Der Verbindungsversuch ist nur erfolgreich, wenn die nag-Mitgliedschaft bestätigt wurde.

Server Isolierung ohne Domänenisolierung

Die Server Isolierung kann auch nur für die Geräte bereitgestellt werden, die teilnehmen müssen. Das Gruppenrichtlinienobjekt auf dem Server unterscheidet sich nicht von dem im vorherigen Absatz für einen Server in einer vorhandenen isolierten Domäne besprochenen. Der Unterschied besteht darin, dass Sie auch ein GPO mit unterstützenden Verbindungssicherheitsregeln für die Clients bereitstellen müssen, die mit dem isolierten Server kommunizieren können sollen. Da diese Geräte Mitglieder des nag sein müssen, kann diese Gruppe auch in einem Sicherheitsgruppenfilter für das Client-GPO verwendet werden. Das Gruppenrichtlinienobjekt muss Regeln enthalten, die die Authentifizierungsanforderungen des isolierten Servers unterstützen.

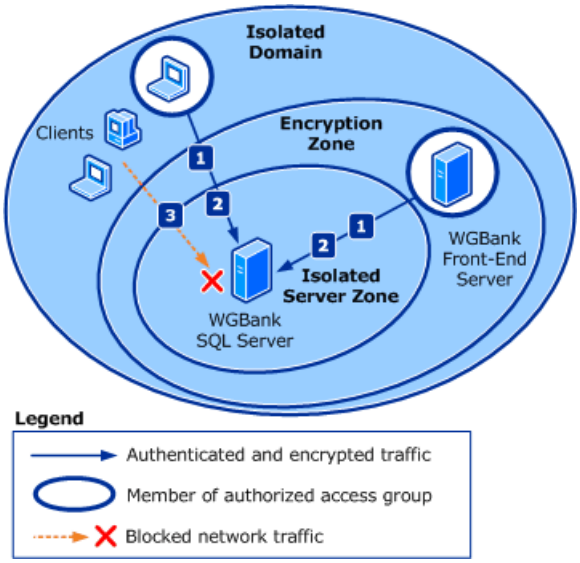
Kurz gesagt: anstatt das Client-GPO auf alle Clients in der Domäne anzuwenden, wenden Sie das Gruppenrichtlinienobjekt nur auf die Mitglieder des nag an.

Wenn Sie nicht über eine Active Directory-Domäne verfügen, können Sie die Verbindungssicherheitsregeln manuell anwenden, ein Netsh-Befehlszeilenskript verwenden oder ein Windows PowerShell-Skript verwenden, um die Konfiguration der Regeln für eine größere Anzahl von Geräten zu automatisieren. Wenn Sie nicht über eine Active Directory-Domäne verfügen, können Sie das KerberosV5-Protokoll nicht verwenden, sondern müssen den Clients und den isolierten Servern Zertifikate zur Verfügung stellen, auf die in den Verbindungssicherheitsregeln Bezug genommen wird.

Entwurfsanforderungen

Neben dem Schutz durch die Firewallregeln und die Domänenisolierung, die in den vorherigen entwurfsbeispielen beschrieben wurden, möchten die Netzwerkadministratoren die Serverisolierung implementieren, um die vertraulichen Daten zu schützen, die auf den Geräten gespeichert sind, auf denen SQL Server ausgeführt wird.

Die folgende Abbildung zeigt den Datenschutz Bedarf für dieses Entwurfsbeispiel.



1. Der Zugriff auf die SQL Server-Geräte muss auf die Computer-oder Benutzerkonten beschränkt sein, die eine geschäftliche Anforderung für den Zugriff auf die Daten aufweisen. Dazu gehören die Dienstkonten, die von den WGBank-Front-End-Servern und Administratoren der SQL Server-Geräte verwendet werden. Darüber hinaus wird der Zugriff nur gewährt, wenn er von einem autorisierten Computer gesendet wird. Die Autorisierung wird durch die Mitgliedschaft in einer Netzwerkzugriffsgruppe (NAG) bestimmt.
2. Der gesamte Netzwerkdatenverkehr zu und von den SQL Server-Geräten muss verschlüsselt werden.
3. Client Geräte oder Benutzer, deren Konten nicht Mitglieder des nag sind, können nicht auf die isolierten Server zugreifen.

Andere Verkehrshinweise:

- Alle Entwurfsanforderungen, die im Beispielabschnitt Firewall-Richtlinienentwurf angezeigt werden, werden weiterhin erzwungen.
- Alle im Abschnitt zum Entwerfen von Domänen Isolierungs Richtlinien gezeigten Entwurfsanforderungen werden weiterhin erzwungen.

Entwurfsdetails

Die Woodgrove Bank verwendet Active Directory-Gruppen und-GPOs zum Bereitstellen der Server Isolationseinstellungen und-Regeln für die Geräte im Netzwerk.

Wie in den zuvor beschriebenen Richtlinienentwurfs Beispielen sind GPOs zum Implementieren der Domäne-Isolierungs Umgebung mit dem Domänencontainer in Active Directory verknüpft, und dann werden WMI-Filter und Sicherheitsgruppenfilter an GPOs angefügt, um sicherzustellen, dass das richtige GPO auf jeden Computer angewendet. Die folgenden Gruppen wurden mit dem Snap-in Active Directory-Benutzer und-Computer erstellt, und alle Geräte, die Windows ausführen, wurden den richtigen Gruppen hinzugefügt.

- **CG_SRVISO_WGBANK_SQL**. Diese Gruppe enthält die Computerkonten für die Geräte, auf denen SQL Server ausgeführt wird. Mitglieder dieser Gruppe erhalten ein GPO mit Sicherheitsregeln für Firewall und Verbindungen, die erfordern, dass nur Benutzer, die Mitglieder der Gruppe CG_NAG_SQL_USERS sind, auf

den Server zugreifen können, und zwar nur, wenn Sie einen Computer verwenden, der Mitglied der Gruppe CG_NAG_SQL_ Computer.

> **Hinweis:** Sie können Ihre GPOs in geschachtelten Gruppen entwerfen. So können Sie beispielsweise die umgrenzungs Gruppe zu einem Mitglied der Gruppe der isolierten Domänen machen, sodass Sie die Firewall und die grundlegenden Einstellungen für die isolierte Domäne über diese geschachtelte Mitgliedschaft erhält, wobei nur die Änderungen durch das Gruppenrichtlinienobjekt für Grenzzonen bereitgestellt werden. Geräte, auf denen ältere Windows-Versionen ausgeführt werden, können jedoch nur eine einzelne IPSec-Richtlinie unterstützen, die gleichzeitig aktiv ist. Die Richtlinien für die einzelnen Gruppenrichtlinienobjekte müssen vollständig (und in hohem Maße redundant miteinander) sein, da Sie Sie in den neueren Versionen von Windows nicht wie möglich überlagern können. Aus Gründen der Einfachheit werden in diesem Leitfaden die Techniken beschrieben, mit denen unabhängige, nicht mehrschichtige Richtlinien erstellt werden. Wir empfehlen, dass Sie ein Skript erstellen und in regelmäßigen Abständen ausführen, das die Mitgliedschaften der Gruppen vergleicht, die sich gegenseitig ausschließen müssen, und Berichte über alle Geräte, die fälschlicherweise mehr als einer Gruppe zugeordnet sind.

Netzwerkzugriffsgruppen werden nicht verwendet, um zu ermitteln, welche GPOs auf einen Computer angewendet werden. Stattdessen legen diese Gruppen fest, welche Benutzer und Geräte auf die Dienste auf dem isolierten Server zugreifen können.

- **CG_NAG_SQL_COMPUTERS**. Diese Netzwerkzugriffsgruppe enthält die Computerkonten, die auf die Geräte zugreifen können, auf denen SQL Server ausgeführt wird, der die WGBank-Daten hostet. Mitglieder dieser Gruppe sind die WGBank-Front-End-Server und einige Clientgeräte, von denen SQL Server-Administratoren auf den Servern arbeiten dürfen.
- **CG_NAG_SQL_USERS**. Diese Netzwerkzugriffsgruppe enthält die Benutzerkonten von Benutzern, die auf die SQL Server-Geräte zugreifen dürfen, die die WGBank-Daten hosten. Zu den Mitgliedern dieser Gruppe gehören das Dienstkonto, das das WGBank-Front-End-Programm für die Ausführung auf seinen Geräten verwendet, und die Benutzerkonten für die Mitglieder des SQL Server-Verwaltungsteams.

> **Hinweis:** Sie können eine einzelne Gruppe für Benutzer-und Computerkonten verwenden. Die Woodgrove Bank hat entschieden, Sie für Klarheit getrennt zu halten.

Wenn die Woodgrove Bank die Serverisolierung ohne Domänenisolierung implementieren möchte, kann die CG_NAG_SQL_COMPUTERS-Gruppe auch als Sicherheitsgruppenfilter für die GPOs angefügt werden, die Verbindungssicherheitsregeln auf die Clientgeräte anwenden. Auf diese Weise verfügen alle Geräte, die für den Zugriff auf den isolierten Server autorisiert sind, auch über die erforderlichen Verbindungssicherheitsregeln.

Sie müssen die Verschlüsselungs fähigen Regeln nicht auf allen Geräten angeben. Stattdessen können Sie Gruppenrichtlinienobjekte erstellen, die nur auf Mitglieder des nag-Objekts angewendet werden, zusätzlich zum standardmäßigen Domänen Isolierungs-GPO, die Verbindungssicherheitsregeln zur Unterstützung der Verschlüsselung enthalten.

Nächster Schritt: Design Beispiel für zertifikatbasierte Isolierungs Richtlinien

Beispiel für den Entwurf einer zertifikatbasierten Isolationsrichtlinie

07.08.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Entwurfsbeispiel wird weiterhin das fiktive Unternehmen Woodgrove Bank verwendet, wie im Beispiel für den Abschnitt Firewall-Richtlinienentwurf, Beispiel für Domänen Isolierungs RichtlinienEntwurf und Beispiel für die Server Isolierungs Richtliniebeschrieben.

Einer der Server, der in der Domäne-Isolierungs Umgebung enthalten sein muss, ist ein Gerät mit UNIX, das andere Informationen für das WGBank-dashboardprogramm bereitstellt, das auf den Clientgeräten ausgeführt wird. Dieses Gerät sendet aktualisierte Informationen an die WGBank-Front-End-Server, sobald diese verfügbar sind, und wird daher als unerwünschter eingehender Datenverkehr für die Geräte angesehen, die diese Informationen erhalten.

Entwurfsanforderungen

Eine mögliche Lösung besteht darin, eine Authentifizierungs Befreiungs Regel in das Gruppenrichtlinienobjekt einzubeziehen, das auf die WGBank-Front-End-Server angewendet wurde. Mit dieser Regel werden die Front-End-Server angewiesen, Datenverkehr vom nicht-Windows-Gerät zu akzeptieren, obwohl es sich nicht authentifizieren kann.

Eine sicherere und die von der Woodgrove Bank ausgewählte Lösung besteht darin, das nicht-Windows-Gerät im Domänen Isolierungs Entwurf einzubeziehen. Da es keiner Active Directory-Domäne beitreten kann, wählte die Woodgrove Bank die zertifikatbasierte Authentifizierung aus. Zertifikate sind kryptografisch geschützte Dokumente, die so verschlüsselt sind, dass ihre Herkunft positiv bestätigt werden kann.

In diesem Fall hat die Woodgrove Bank die Active Directory-Zertifikatdienste verwendet, um das entsprechende Zertifikat zu erstellen. Sie haben möglicherweise auch ein Zertifikat von einer kommerziellen Zertifizierungsstelle von Drittanbietern erworben und installiert. Anschließend wurden die Gruppenrichtlinien zum Bereitstellen des Zertifikats für die Front-End-Server verwendet. Zu den auf die Front-End-Server angewendeten GPOs gehören auch aktualisierte Verbindungssicherheitsregeln, die zusätzlich zur KerberosV5-Authentifizierung zertifikatbasierte Authentifizierung zulassen. Anschließend wurde das Zertifikat auf dem UNIX-Server manuell installiert.

Der UNIX-Server ist mithilfe der Tools, die vom Hersteller des Betriebssystems bereitgestellt werden, mit Firewall- und IPsec-Verbindungssicherheitsregeln konfiguriert. Diese Regeln geben an, dass die Authentifizierung mithilfe des Zertifikats durchgeführt wird.

Die Erstellung der IPsec-Verbindungssicherheitsregeln für ein nicht-Windows-Gerät sprengt den Rahmen dieses Dokuments, aber die Unterstützung für ein Zertifikat, das zur Authentifizierung eines solchen nicht-Windows-Geräts mithilfe der IPSec-Standardprotokolle verwendet werden kann, ist Gegenstanddieser Design.

Das nicht-Windows-Gerät kann basierend auf den auf das Gerät angewendeten IPSec-Regeln effektiv zu einem Mitglied der Grenz Zone oder zur Verschlüsselungszone gemacht werden. Die einzige Einschränkung besteht darin, dass die vom UNIX-Gerät unterstützten Hauptmodus-und Schnellmodus-Verschlüsselungsalgorithmen auch von den Windows-basierten Geräten unterstützt werden müssen, mit denen Sie kommuniziert.

Andere Verkehrshinweise:

- Keine der Funktionen der anderen in diesem Leitfaden besprochenen Designs wird durch die Verwendung der Zertifikatauthentifizierung durch ein nicht-Windows-Gerät beeinträchtigt.

Entwurfsdetails

Die Woodgrove Bank verwendet Active Directory-Gruppen und-GPOs, um die Domänen Isolationseinstellungen und-Regeln für die Geräte in Ihrer Organisation bereitzustellen.

Die Einbeziehung von einem oder mehreren nicht-Windows-Geräten in das Netzwerk erfordert nur eine einfache Ergänzung der GPOs für Geräte, die mit dem nicht-Windows-Gerät kommunizieren müssen. Der Zusatz ermöglicht die zertifikatbasierte Authentifizierung zusätzlich zur Active Directory-unterstützten KerberosV5-Authentifizierung. Dazu sind keine neuen Regeln erforderlich, sondern nur das Hinzufügen einer zertifikatbasierten Authentifizierung als Option zu den vorhandenen Regeln.

Wenn mehrere Authentifizierungsmethoden zur Verfügung stehen, vereinbaren zwei Verhandlungs Geräte den ersten in den Listen, die übereinstimmen. Da die Mehrheit der Geräte im Netzwerk der Woodgrove Bank Windows ausführt, wird KerberosV5 in den Regeln als erste Authentifizierungsmethode aufgeführt. Die zertifikatbasierte Authentifizierung wird als alternativer Authentifizierungstyp hinzugefügt.

Mit dem Snap-in "Active Directory-Benutzer und-Computer" hat die Woodgrove Bank eine Gruppe mit dem Namen "NAG_COMPUTER_WGBUNIX." erstellt. Sie haben dann die Geräte Konten dieser Gruppe für Windows-Geräte hinzugefügt, die mit den nicht-Windows-Geräten kommunizieren müssen. Wenn alle Geräte in der isolierten Domäne auf die nicht-Windows-Geräte zugreifen müssen, kann die Gruppe " **Domänencomputer** " der Gruppe als Mitglied hinzugefügt werden.

Die Woodgrove Bank hat dann ein GPO erstellt, das das Zertifikat enthält, und dann Sicherheitsgruppenfilter an das Gruppenrichtlinienobjekt angefügt, das Berechtigungen für Lesen und Anwenden nur für Mitglieder der NAG_COMPUTER_WGBUNIX-Gruppe ermöglicht. Das Gruppenrichtlinienobjekt platziert das Zertifikat im Zertifikatspeicher des **lokalen Computers/Personal/Zertifikate** . Das verwendete Zertifikat muss an ein Zertifikat zurück gekettet sein, das sich im Speicher der **vertrauenswürdigen Stammzertifizierungsstellen** auf dem lokalen Gerät befindet.

Nächster Schritt: Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategie

Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategie

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Wenn Sie das effektivste Design für den Schutz des Netzwerks auswählen möchten, müssen Sie Zeit damit verbringen, wichtige Informationen zu Ihrer aktuellen Computerumgebung zu sammeln. Sie müssen ein gutes Verständnis davon haben, welche Aufgaben die Geräte im Netzwerk ausführen, und wie Sie diese Aufgaben mit dem Netzwerk ausführen. Sie müssen den Netzwerkdatenverkehr verstehen, der von den auf den Geräten ausgeführten Programmen generiert wird.

- Sammeln der erforderlichen Informationen
- Ermitteln des vertrauenswürdigen Zustands Ihrer Geräte

Die von Ihnen gesammelten Informationen werden Ihnen bei der Beantwortung der folgenden Fragen helfen. Die Antworten werden Ihnen helfen, Ihre Sicherheitsanforderungen zu verstehen und das Design auszuwählen, das diesen Anforderungen am besten entspricht. Die Informationen werden Ihnen auch helfen, wenn es Zeit für die Bereitstellung Ihres Entwurfs ist, indem Sie Ihnen helfen, eine Bereitstellungsstrategie zu erstellen, die kostengünstig und Ressourcen effizient ist. Sie wird Ihnen dabei helfen, die voraussichtlichen Kosten für die Implementierung des Entwurfs zu projizieren und zu rechtfertigen.

- Welcher Datenverkehr muss immer zulässig sein? Was sind die Merkmale des Netzwerkverkehrs, die von den Geschäftsprogrammen generiert und genutzt werden?
- Welcher Datenverkehr muss immer blockiert werden? Verfügt Ihre Organisation über Richtlinien, die die Verwendung bestimmter Programme verbieten? Wenn ja, welche Merkmale hat der Netzwerkverkehr, der von den verbotenen Programmen generiert und verbraucht wird?
- Welcher Datenverkehr im Netzwerk kann nicht durch IPSec geschützt werden, da die Geräte oder Geräte, die den Datenverkehr senden oder empfangen, IPSec nicht unterstützen?
- Wird für jeden Netzwerkdatenverkehr die Standardkonfiguration der Firewall (alle nicht angeforderten eingehenden Netzwerkdatenverkehr blockieren, allen ausgehenden Datenverkehr zulassen) den Datenverkehr nach Bedarf zulassen oder blockieren?
- Verfügen Sie über eine Active Directory-Domäne (oder eine Gesamtstruktur von vertrauenswürdigen Domänen), der alle Ihre Geräte beigetreten sind? Wenn dies nicht der Fall ist, können Sie die Gruppenrichtlinien nicht für eine einfache Massenbereitstellung Ihrer Firewall-und Verbindungssicherheitsregeln verwenden. Sie können auch die KerberosV5-Authentifizierung, die alle Domänenclients verwenden können, nicht einfach nutzen.
- Welche Geräte müssen unerwünschte eingehende Verbindungen von Geräten akzeptieren können, die nicht zur Domäne gehören?
- Welche Geräte enthalten Daten, die verschlüsselt werden müssen, wenn Sie mit einem anderen Computer ausgetauscht werden?
- Welche Geräte enthalten vertrauliche Daten, auf die der Zugriff auf speziell autorisierte Benutzer und

Geräte beschränkt sein muss?

- Verfügt Ihre Organisation über bestimmte Netzwerkproblem Behandlungsgeräte oder-Geräte (wie Protokollanalysatoren), denen ein unbegrenzter Zugriff auf die Geräte im Netzwerk gewährt werden muss, wobei die Firewall im wesentlichen umgangen wird?

In diesem Leitfaden wird beschrieben, wie Sie Ihre Gruppen und GPOs für eine Umgebung mit einer Kombination aus Betriebssystemen planen. Details finden Sie im Abschnitt Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen weiter unten in diesem Leitfaden.

Als nächstes: Sammeln der erforderlichen Informationen

Sammeln der erforderlichen Informationen

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Bevor Sie den Planungsprozess für eine Windows Defender-Firewall mit erweiterter Sicherheits Bereitstellung starten, müssen Sie aktuelle Informationen zu dem Netzwerk, den Verzeichnisdiensten und den Geräten, die bereits in der Organisation bereitgestellt wurden, sammeln und analysieren. Mithilfe dieser Informationen können Sie ein Design erstellen, das alle möglichen Elemente der vorhandenen Infrastruktur berücksichtigt. Wenn die gesammelten Informationen nicht korrekt sind, kann es zu Problemen kommen, wenn während der Implementierung keine Geräte und Geräte auftreten, die während der Planungsphase nicht berücksichtigt wurden.

Überprüfen Sie die einzelnen der folgenden Themen, um Anleitungen zu den Arten von Informationen zu erhalten, die Sie sammeln müssen:

- Sammeln von Informationen zur aktuellen Netzwerkinfrastruktur
- Sammeln von Informationen zur Active Directory-Bereitstellung
- Sammeln von Informationen zu Ihren Geräten
- Sammeln anderer relevanter Informationen

Sammeln von Informationen zur aktuellen Netzwerkinfrastruktur

04.12.2019 • 8 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Der vielleicht wichtigste Aspekt bei der Planung der Windows Defender-Firewall mit erweiterter Sicherheits Bereitstellung ist die Netzwerkarchitektur, da IPSec auf dem Internet Protokoll selbst basiert. Ein unvollständiges oder ungenaues Verständnis des Netzwerks kann verhindern, dass Windows Defender-Firewall-Lösungen erfolgreich sind. Das Grundlegendes zu Subnetz-Layout, IP-Adressierungsschemas und Datenverkehrsmustern ist Teil dieser Anstrengung, aber die genaue Dokumentation der folgenden Komponenten ist für die Durchführung der Planungsphase dieses Projekts wichtig:

- **Netzwerksegmentierung**. Dazu gehören IP-Adressierungs Karten, die zeigen, wie Ihre Router die einzelnen Netzwerksegmente voneinander trennen. Sie enthält Informationen dazu, wie die Router konfiguriert sind und welche Sicherheitsfilter Sie für den Netzwerkdatenverkehr durchlaufen.
- Netzwerkadressübersetzung (NAT). NAT ist ein Mittel zum Trennen von Netzwerksegmenten mithilfe eines Geräts, das alle IP-Adressen auf einer Seite des Geräts einer einzelnen IP-Adresse zuordnet, auf die auf der anderen Seite zugegriffen werden kann.
- Netzwerkinfrastruktur Geräte. Dazu gehören Router, Switches, Hubs und andere Netzwerkgeräte, mit denen die Kommunikation zwischen den Geräten im Netzwerk möglich ist.
- **Aktuelles Netzwerkverkehrs Modell** Dies umfasst die Menge und die Merkmale des Netzwerkverkehrs, der über Ihr Netzwerk fließt.
- Intrusion Detection System (IDs)-Geräte. Sie müssen ermitteln, ob Sie über IDs-Geräte in Ihrem Netzwerk verfügen, die sich möglicherweise negativ auf eine Verschlüsselung auswirken, die in einer Verschlüsselungs Zone eingeführt wurde.

Das Ziel besteht darin, genügend Informationen zur Verfügung zu haben, um eine Ressource zusätzlich zum physikalischen Standort über Ihren Netzwerkstandort zu identifizieren.

Verwenden Sie kein komplexes und unzureichend dokumentiertes Netzwerk als Ausgangspunkt für das Design, da es zu viele nicht identifizierte Bereiche hinterlassen kann, die wahrscheinlich Probleme während der Implementierung verursachen.

Dieser Leitfaden hilft Ihnen, die relevantesten Informationen für die Planung der Windows Defender-Firewall-Implementierung zu erhalten, versucht aber nicht, andere Probleme wie TCP/IP-Adressierung oder VLAN-Segmentierung (virtuelles lokales Netzwerk) zu beheben.

Netzwerksegmentierung

Wenn Ihre Organisation nicht die aktuelle Netzwerkarchitektur dokumentiert und als Referenz verfügbar ist, sollte diese Dokumentation so schnell wie möglich abgerufen werden, bevor Sie den Entwurf und die Bereitstellung fortsetzen. Wenn die dokumentierten Informationen nicht aktuell sind oder vor kurzem nicht überprüft wurden, haben Sie zwei Möglichkeiten:

- Akzeptieren Sie, dass das Fehlen genauer Informationen zu Risiken für das Projekt führen kann.
- Führen Sie ein Ermittlungs Projekt durch, entweder durch manuelle Prozesse oder mithilfe von Tools für die Netzwerkanalyse, die die Informationen bereitstellen können, die Sie zum Dokumentieren der aktuellen Netzwerktopologie benötigen.

Obwohl die erforderlichen Informationen auf viele verschiedene Arten dargestellt werden können, ist eine Reihe von schematischen Diagrammen oft die effektivste Methode, um die aktuelle Netzwerkkonfiguration zu illustrieren und zu verstehen. Berücksichtigen Sie beim Erstellen von Netzwerkdiagrammen nicht zu viele Informationen. Verwenden Sie bei Bedarf mehrere Diagramme, die unterschiedliche Detailebenen aufweisen. Verwenden Sie ein Diagramm auf oberster Ebene, in dem die wichtigsten Websites, aus denen das Netzwerk Ihrer Organisation besteht, veranschaulicht werden, und teilen Sie dann jede Website in einem detaillierteren Diagramm auf, in dem eine tiefere Detailebene erfasst wird. Fahren Sie fort, bis Sie die einzelnen IP-subnetebene erreicht haben, und weisen Sie so die Möglichkeit auf, den Netzwerkstandort jedes Geräts in Ihrer Organisation zu identifizieren.

Während dieses Vorgangs finden Sie möglicherweise einige Netzwerkanwendungen und Dienste, die nicht mit IPSec kompatibel sind. IPSec unterbricht beispielsweise die netzwerkbasierte Priorisierung und die Port/Protokoll-basierte Datenverkehrsverwaltung. Wenn die Datenverkehrsverwaltung oder-Priorisierung auf Ports oder Protokoll basieren muss, muss der Host selbst in der Lage sein, jede Verkehrsverwaltung oder Priorisierung durchzuführen.

Weitere Beispiele für Inkompatibilität sind:

- Cisco Netflow auf Routern kann keine Pakete zwischen IPSec-Mitgliedern basierend auf Protokoll oder Port analysieren.
- Router-basierte QoS (Quality of Service) kann keine Ports oder Protokolle verwenden, um den Datenverkehr zu priorisieren. Die Verwendung von Firewallregeln, die IP-Adressen angeben, um den Datenverkehr zu priorisieren, ist jedoch von dieser Einschränkung von QoS nicht betroffen. Beispielsweise funktioniert eine Regel, die besagt, dass "von jedem für jeden, der Port 80 priorisiert," nicht funktioniert, aber eine Regel, die besagt, dass "von einer beliebigen Person zu 10.0.1.10 priorisieren" funktioniert.
- Gewichtete Fair Queuing-und andere Flow-basierte Router-Datenverkehrs Prioritäts Methoden können fehlschlagen.
- Geräte, die das IP-Protokoll 50 nicht unterstützen oder zulassen, der Port, der vom Encapsulating Security Payload (ESP) verwendet wird.
- Router-Zugriffssteuerungslisten (ACLs) können keine Protokoll-und Port Felder in ESP-verschlüsselten Paketen untersuchen, und daher werden die Pakete gelöscht. ACLs, die nur auf IP-Adressen basieren, werden wie gewohnt weitergeleitet. Wenn das Gerät keine ESP-Analyse durchführt, werden alle ACLs, die Port-oder Protokollregeln angeben, nicht für die ESP-Pakete verarbeitet. Wenn das Gerät über einen ESP-Parser verfügt und Verschlüsselung verwendet, werden ACLs, die Port-oder Protokollregeln angeben, nicht für die ESP-Pakete verarbeitet.
- Netzwerküberwachungstools können keine ESP-Pakete analysieren, die nicht verschlüsselt (ESP-null) sind.

> **Hinweis:** Microsoft Message Analyzer kann bei der Problembehandlung von nicht verschlüsselten IPSec-Paketen helfen. Die neueste Version von Message Analyzer steht im Microsoft Download Centerzur Verfügung.

Netzwerkadressübersetzung (NAT)

IPSec-NAT-Traversal (NAT-T) ermöglicht IPSec-Peers hinter NATs, das vorhanden sein von NATs zu erkennen, IPSec-Sicherheitszuordnungen auszuhandeln und ESP-geschützte Daten zu senden, obwohl sich die Adressen in den IPSec-geschützten IPv4-Paketen ändern. IPSec NAT-T unterstützt die Verwendung von AH auf NAT-Geräten

nicht.

Netzwerkinfrastruktur Geräte

Die Geräte, aus denen sich die Netzwerkinfrastruktur (Router, Switches, Load-Balancer und Firewalls), müssen nach der Implementierung der Lösung über IPSec kommunizieren können. Aus diesem Grund müssen Sie die folgenden Merkmale dieser Netzwerkgeräte untersuchen, um sicherzustellen, dass Sie die technischen und physikalischen Anforderungen des Entwurfs erfüllen können:

- **Marke/Modell**. Mithilfe dieser Informationen können Sie die vom Gerät unterstützten Features ermitteln. Überprüfen Sie außerdem die BIOS-Version oder Software, die auf dem Gerät ausgeführt wird, um sicherzustellen, dass IPSec unterstützt wird.
- Die **Menge an Arbeitsspeicher**. Diese Informationen sind hilfreich, wenn Sie die Kapazität oder die Auswirkungen von IPSec auf das Gerät analysieren.
- **Datenverkehrsanalyse**. Informationen wie Spitzenauslastung und tägliche orweekly-Trends sind hilfreich. Mithilfe dieser Informationen können Sie einen Basisplan-Schnappschuss des Geräts und dessen Verwendung im Laufe der Zeit bereitstellen. Wenn nach der Implementierung von IPSec Probleme auftreten, können Sie anhand der Informationen ermitteln, ob sich die Ursache auf eine größere Auslastung des Geräts bezieht.
- **Router-ACLs, die IPSec direkt beeinflussen**. ACLs wirken sich direkt auf die Funktion bestimmter Protokolle aus. Das Blockieren des KerberosV5-Protokolls (UDP und TCP-Port 88) oder IP-Protokoll 50 oder 51 verhindert beispielsweise, dass IPSec funktioniert. Geräte müssen auch so konfiguriert werden, dass IKE-Datenverkehr (UDP-Port 500) bei Verwendung von NAT-T (UDP-Port 4500) zulässig ist.
- **Netzwerke/Subnetze, die mit Geräteschnittstellen verbunden**sind. Diese Informationen bieten ein optimales Bild davon, wie das interne Netzwerk aussieht. Das Definieren der Begrenzung von Subnetzen auf der Grundlage eines Adressbereichs ist unkompliziert und hilft zu erkennen, ob andere Adressen entweder nicht verwaltet oder für das interne Netzwerk fremd sind (beispielsweise IP-Adressen im Internet).
- **VLAN-Segmentierung**. Wenn Sie feststellen, wie VLANs im Netzwerk implementiert werden, können Sie Datenverkehrsmuster und Sicherheitsanforderungen besser verstehen und dann helfen, zu bestimmen, wie IPSec diese Anforderungen erweitern oder stören kann.
- **Die maximale Größe der Übertragungseinheit (MTU) auf der Geräteschnittstelle (n)**. Die MTU definiert das größte Datagramm, das auf einer bestimmten Schnittstelle übertragen werden kann, ohne dass es für die Übertragung in kleinere Abschnitte unterteilt wird (ein Prozess, der auch als *Fragmentierung*bezeichnet wird). Bei der IPSec-Kommunikation ist die MTU notwendig, um zu antizipieren, wann eine Fragmentierung stattfindet. Die Paketfragmentierung muss vom Router für Internet Security Association und ISAKMP (Key Management Protocol) nachverfolgt werden. IPsec konfiguriert die MTU-Größe für die Sitzung auf die mindestens erkannte MTU-Größe entlang des verwendeten Kommunikationspfads und legt dann das Bit "nicht fragmentieren" (DF-Bit) auf 1 fest.

  > **Hinweis:** wenn die Pfad-MTU-Erkennung (PMTU) aktiviert ist und ordnungsgemäß funktioniert, müssen Sie die MTU-Größe nicht auf Geräteschnittstellen sammeln. Obwohl Quellen wie der Windows-Server2003-Härtungs Leit Faden die Deaktivierung der PMTU-Erkennung empfehlen, muss Sie für IPSec aktiviert sein, damit Sie ordnungsgemäß funktioniert.

- **Intrusion Detection System (IDs) wird verwendet**. Ihre IDs müssen über einen IPSec-kompatiblen Parser verfügen, um ESP-Pakete zu erkennen. Wenn die IDs keinen solchen Parser besitzen, kann Sie nicht feststellen, ob Daten in diesen Paketen verschlüsselt sind.

Nachdem Sie diese Informationen abgerufen haben, können Sie schnell ermitteln, ob Sie die Geräte aktualisieren

müssen, um die Anforderungen des Projekts zu unterstützen, die ACLs zu ändern oder andere Maßnahmen zu ergreifen, um sicherzustellen, dass die Geräte die erforderlichen Lasten verarbeiten können.

Aktuelles Netzwerkverkehrs Modell

Nachdem Sie die Adressierungs-und Netzwerkinfrastruktur Informationen erfasst haben, besteht der nächste Schritt darin, den Kommunikationsfluss zu untersuchen. Wenn beispielsweise eine Abteilung wie Personal Resources (HR) mehrere Gebäude umfasst und Sie die Serverisolierung mit Verschlüsselung verwenden möchten, um Informationen in dieser Abteilung zu schützen, müssen Sie wissen, wie diese Gebäude verbunden sind, um den Grad der "Vertrauensstellung" zu ermitteln. in der Verbindung platzieren. Ein hoch gesichertes Gebäude, das durch ein ungeschütztes Kabel mit einem anderen Gebäude verbunden ist, das nicht gesichert ist, kann durch Abhör- oder Informationswiedergabe Angriffe beeinträchtigt werden. Wenn ein solcher Angriff als Bedrohung angesehen wird, kann IPSec durch eine starke gegenseitige Authentifizierung und Datenverkehrs Verschlüsselung für vertrauenswürdige Hosts helfen. IPSec ermöglicht eine sicherere Kommunikation über nicht vertrauenswürdige Links wie das Internet.

Wenn Sie den Datenverkehrs Fluss untersuchen, schauen Sie sich genau an, wie alle verwalteten und nicht verwalteten Geräte interagieren. Dazu gehören nicht-Windows-basierte Geräte mit Linux, UNIX und Macintosh. Stellen Sie sich folgende Fragen:

- Erfolgen bestimmte Kommunikationen auf Port-und Protokollebene, oder gibt es viele Sitzungen zwischen denselben Hosts in vielen Protokollen?
- Wie kommunizieren Server und Clients miteinander?
- Gibt es Sicherheitsgeräte oder Projekte, die derzeit implementiert oder geplant sind, die sich auf eine Isolierungs Bereitstellung auswirken könnten? Wenn Sie beispielsweise die Windows Defender-Firewall auf Ihren Geräten verwenden, um bestimmte Ports wie UDP 500 zu "Sperren", schlagen IKE-Verhandlungen fehl.

Einige der häufiger verwendeten Anwendungen und Protokolle sind wie folgt:

- **NetBIOS über TCP/IP (NetBT) und Server-Nachrichtenblock (SMB)**. In einem LAN ist es üblich, dass die Ports 137, 138 und 139 für NetBT und Port 445 für SMB aktiviert sind. Diese Anschlüsse bieten Dienste für NetBIOS-Namensauflösungen und andere Funktionen. Leider können auch *Null-Sitzungen*erstellt werden. Eine NULL-Sitzung ist eine Sitzung, die auf einem Host eingerichtet wird, der nicht den Sicherheitskontext eines bekannten Benutzers oder einer bekannten Entität verwendet. Häufig sind diese Sitzungen anonym.
- **Remote Prozeduraufruf (RPC)**. RPC funktioniert durch lauschen auf einem Port, der als *Endpunktzuordnung*bezeichnet wird, TCP-Port 135. Die Antwort auf eine Abfrage für diesen Port ist eine Anweisung zum beginnen der Kommunikation an einem anderen Port im ephemeren Bereich (Ports, die über 1024 nummeriert sind). In einem Netzwerk, das von Firewalls segmentiert ist, stellt die RPC-Kommunikation eine Herausforderung für die Konfiguration dar, da dies bedeutet, den RPC-Listener-Port und alle Ports größer als 1024 zu öffnen. Wenn Sie so viele Ports öffnen, wird die Angriffsfläche des gesamten Netzwerks erhöht und die Effektivität der Firewalls verringert. Da viele Anwendungen von RPC für grundlegende Funktionen abhängen, müssen alle Firewall-und Verbindungssicherheitsrichtlinien die RPC-Anforderungen berücksichtigen.
- **Anderer Datenverkehr**. Die Windows Defender-Firewall kann Ihnen helfen, die Übertragung zwischen Geräten zu sichern, indem Sie zusätzlich zur Verschlüsselung der enthaltenen Daten die Authentifizierung der Pakete bereitstellt. Wichtig ist, zu erkennen, was geschützt werden muss, und die Bedrohungen, die gemildert werden müssen. Untersuchen und modellieren Sie weitere Datenverkehrs-oder Datenverkehrstypen, die gesichert werden müssen.

Weiter: Sammeln von Informationen zu Ihrer Active Directory-Bereitstellung

Sammeln von Informationen zur Active Directory-Bereitstellung

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Active Directory ist ein weiterer wichtiger Punkt, über den Sie Informationen sammeln müssen. Sie müssen die Gesamtstruktur verstehen. Dazu gehören Domänenlayout, Architektur der Organisationseinheit (OU) und Standorttopologie. Mithilfe dieser Informationen können Sie wissen, wo die Geräte aktuell gespeichert sind, deren Konfiguration und die Auswirkungen von Änderungen an Active Directory, die sich aus der Implementierung der Windows Defender-Firewall mit erweiterter Sicherheit ergeben. Überprüfen Sie die folgende Liste, um die erforderlichen Informationen zu erhalten:

- **Namen und Anzahl der Gesamtstrukturen** Die Gesamtstruktur (nicht die Domäne) ist die Sicherheitsgrenze in einer Active Directory-Implementierung. Sie müssen die aktuelle Active Directory-Architektur kennen, um die effektivste Strategie für die Bereitstellung Ihrer Firewall-und Verbindungssicherheitsregeln mithilfe von Gruppenrichtlinien zu ermitteln. Darüber hinaus können Sie wissen, welche Geräte isoliert werden können und wie Sie das erforderliche Maß an Isolierung optimal erreichen.

- **Namen und die Anzahl der Domänen**. Bei der Authentifizierung in der Server-und Domänenisolierung wird der IKE-Aushandlungsprozess mit dem KerberosV5-Protokoll verwendet. Dieses Protokoll geht davon aus, dass Geräte Domänenmitglieder sind.

- **Anzahl und Typen von Vertrauensstellungen**. Vertrauensstellungen wirken sich auf die logischen Grenzen der Domänenisolierung aus und definieren, ob die IKE-Aushandlung zwischen Geräten in verschiedenen Active Directory-Domänen erfolgen kann.

- **Namen und Anzahl der Websites**. Die Websitearchitektur wird normalerweise an der Netzwerktopologie ausgerichtet. Wenn Sie wissen, wie Websites in Active Directory definiert werden, können Sie Einblicke in die Replikation und weitere Details vermitteln. Websitearchitektur kann ein besseres Verständnis der aktuellen Active Directory-Bereitstellung bieten.

- **OU-Struktur**. OUs sind logische Konstrukte und können daher so geformt werden, dass Sie vielen unterschiedlichen Anforderungen und Zielen entsprechen. Die OU-Struktur ist ein idealer Ort, um zu untersuchen, wie Gruppenrichtlinien aktuell verwendet werden und wie die OUs angeordnet sind. Sie müssen keine bereits implementierte OU-Struktur neu entwerfen, um Firewall-und Verbindungssicherheitsrichtlinien effektiv bereitzustellen, doch ein Verständnis der Struktur hilft Ihnen, zu wissen, welche WMI-oder Gruppenfilterung erforderlich ist, um die einzelnen Gruppenrichtlinienobjekte auf die richtigen Geräte anzuwenden. .

- **Vorhandene IPSec-Richtlinie**. Da dieses Projekt in der Implementierung der IPSec-Richtlinie gipfelt, müssen Sie wissen, wie das Netzwerk zurzeit IPSec verwendet (wenn überhaupt). Windows Defender-Firewall-Verbindungssicherheitsregeln für Windows-Versionen vor Windows Vista und Windows Server 2008 sind mit früheren Windows-Versionen nicht kompatibel. Wenn Sie bereits IPSec-Richtlinien auf Geräten mit WindowsXP und Windows Server2003 in Ihrer Organisation bereitgestellt haben, müssen Sie sicherstellen, dass die von Ihnen bereitgestellten neuen IPSec-Richtlinien Geräte mit der alten oder neuen IPSec-Richtlinie für die Kommunikation mit einander aktivieren.

Nächster Schritt: Sammeln von Informationen zu Ihren Geräten

Sammeln von Informationen zu Ihren Geräten

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Einer der wichtigsten Vorteile bei der Durchführung eines Ressourcen Ermittlungs Projekts ist die große Menge an Daten, die über die Client-und Server Geräte im Netzwerk abgerufen werden. Wenn Sie mit dem Entwerfen und Planen Ihrer Isolierungs Zonen beginnen, müssen Sie Entscheidungen treffen, die genaue Informationen über den Zustand aller Hosts erfordern, um sicherzustellen, dass Sie IPSec wie geplant verwenden können.

Erfassen Sie die folgenden Informationen auf jedem Gerät:

- **Computer Name** Dieser Name ist der NetBIOS-oder DNS-Name des Geräts, der das Gerät im Netzwerk identifiziert. Da ein Gerät über mehr als eine Medienzugriffssteuerung (Mac) oder eine IP-Adresse verfügen kann, ist der Name des Geräts eines der Kriterien, die zum Ermitteln der Eindeutigkeit im Netzwerk verwendet werden können. Da Gerätenamen unter bestimmten Umständen dupliziert werden können, sollte die Eindeutigkeit nicht als absolut gelten.

- **IP-Adresse für jeden Netzwerkadapter**. Die IP-Adresse ist die Adresse, die mit der Subnetzmaske verwendet wird, um einen Host im Netzwerk zu identifizieren. Eine IP-Adresse ist keine effektive Methode, um ein Objekt zu identifizieren, da es sich häufig ändern kann.

- **Betriebssystem, Service Pack und Hotfix-Versionen**. Die Version des Betriebssystems ist ein entscheidender Faktor bei der Bestimmung der Fähigkeit eines Hosts, mithilfe von IPSec zu kommunizieren. Darüber hinaus ist es wichtig, den aktuellen Status von Service Packs und Updates zu überwachen, die möglicherweise installiert werden, da diese häufig verwendet werden, um festzustellen, ob die Mindestanforderungen für die Sicherheit erfüllt sind.

- **Domänenmitgliedschaft**. Diese Informationen werden verwendet, um zu ermitteln, ob ein Gerät eine IPSec-Richtlinie aus Active Directory abrufen kann oder ob eine lokale IPSec-Richtlinie verwendet werden muss.

- **Physischer Standort**. Diese Informationen sind nur der Standort des Geräts in Ihrer Organisation. Sie kann verwendet werden, um zu ermitteln, ob ein Gerät an einer bestimmten Isolierungsgruppe basierend auf seinem Standort oder dem Standort der Geräteteil nehmen kann, mit denen es regelmäßig kommuniziert.

- **Hardwaretyp oder-Rolle** Einige Tools, die die Hostermittlung durchführen, können diese Informationen bereitstellen, indem Sie die Hardwareinformationen Abfragen und Anwendungen ausführen, um deren Typ zu ermitteln, beispielsweise Server, Workstation oder tragbares Gerät. Mithilfe dieser Informationen können Sie die geeignete IPSec-Richtlinie ermitteln, die zugewiesen werden soll, ob ein bestimmtes Gerät isoliert teilnehmen kann und in welcher Isolierungsgruppe das Gerät eingeschlossen werden soll.

Nachdem Sie alle diese Informationen gesammelt und in einer Datenbank konsolidiert haben, führen Sie regelmäßige Ermittlungsbemühungen durch, um die Informationen aktuell zu halten. Sie benötigen ein vollständiges und Aktuelles Bild der verwalteten Hosts in ihren Netzwerken, um einen Entwurf zu erstellen, der den Anforderungen Ihrer Organisation entspricht.

Sie können verschiedene Methoden verwenden, um Daten von den Hosts im Netzwerk zu sammeln. Diese Methoden sind von Highend-voll automatisierten Systemen bis hin zur vollständigen manuellen Datenerfassung.

Im Allgemeinen wird die Verwendung automatisierter Methoden zum Sammeln von Daten über manuelle Methoden aus Gründen der Geschwindigkeit und Genauigkeit bevorzugt.

Automatisierte Ermittlung

Mithilfe eines automatisierten Überwachungsnetzwerk-Verwaltungssystems erhalten Sie wertvolle Informationen zum aktuellen Zustand der IT-Infrastruktur.

Manuelle Ermittlung

Der größte Unterschied zwischen manuellen Ermittlungsmethoden und automatisierten Methoden ist die Zeit.

Sie können Windows PowerShell verwenden, um eine Skriptdatei zu erstellen, die die Systemkonfigurationsinformationen erfassen kann. Weitere Informationen finden Sie unter Windows PowerShell-Skripterstellung.

Unabhängig davon, ob Sie eine automatische, manuelle oder hybride Option zum Sammeln der Informationen verwenden, ist eines der größten Probleme, die zu Problemen beim Entwurf führen können, die Erfassung der Änderungen zwischen dem ursprünglichen Inventur Scan und dem Zeitpunkt, zu dem die Implementierung bereit ist, zu starten. Stellen Sie nach Abschluss des ersten Scans sicher, dass alle zusätzlichen Änderungen aufgezeichnet werden müssen und die Updates im Inventar notiert sind.

Diese Bestandsaufnahme ist für die Planung und Implementierung Ihres Windows Defender-Firewall-Designs von entscheidender Bedeutung.

Nächster Schritt: Sammeln anderer relevanter Informationen

Sammeln anderer relevanter Informationen

07.08.2019 • 6 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Thema werden einige andere Dinge erläutert, die Sie untersuchen sollten, um festzustellen, ob diese zu Komplikationen bei der Bereitstellung von Windows Defender Firewall mit erweiterten Sicherheitsrichtlinien in Ihrer Organisation führen.

Überlegungen zur Kapazität

Da IPSec mathematisch aufwändige kryptografische Techniken verwendet, kann dies einen erheblichen Overhead auf einem Gerät beanspruchen. Zu beobachtende Bereiche:

- **Verschlüsselung.** Möglicherweise verwenden Sie 256-Bit Advanced Encryption Standard (AES-256) und 384-Bit Secure Hash Algorithm (SHA-384), um die Integrität in Situationen zu überprüfen, die die stärkste verfügbare Verschlüsselung und den wichtigsten Exchange-Schutz erfordern. Wenn Sie über NICs verfügen, die die IPSec-Aufgaben Entlastung unterstützen, können Sie die Auswirkungen der Verschlüsselung auf den Netzwerkdurchsatz reduzieren. Weitere Informationen finden Sie unter IPSec-Aufgaben Entlastung.
- **Security Association (SA)-Aushandlung.** Sie können eine kürzere Lebensdauer für die Hauptmodus-Sicherheitszuordnung wie drei Stunden verwenden, doch müssen Sie möglicherweise Kompromisse vornehmen. Da jede Hauptmodus-Sicherheitszuordnung ungefähr 5 kByte RAM umfasst, können Situationen, in denen ein Server Zehntausende von gleichzeitigen Verbindungen einnimmt, zu einer über Auslastung führen.
- **NAT-Geräte.** Wie bereits zuvor erläutert, erlaubt NAT keine AH-Konversationen (Authentication Header) zwischen Hosts. Wenn NAT-Geräte im internen Netzwerk vorhanden sind, muss ESP anstelle von AH ausgewählt werden.
- **Switches und Router.** Die ordnungsgemäße Kapazitätsplanung für die Implementierung von IPSec basiert eher auf gründlichen Tests und erwarteten Datenverkehrslasten als exakten Berechnungen. Möglicherweise müssen Sie Switches oder Router, die derzeit die Verwendung von 75 Prozent überschreiten, aktualisieren oder neu konfigurieren, um erhöhten Datenverkehr auf dem Gerät zu ermöglichen, und dennoch eine zusätzliche Nutzung für Platz Ausbrüche bereitstellen.
- **Weitere Faktoren.** Dazu zählen die CPU-Auslastung auf Netzwerkinfrastruktur Servern, ein höherer Overhead auf Servern und Workstations mit IPSec (insbesondere Server, da diese normalerweise mehr Hauptmodus-SAS als Clients enthalten) und erhöhte Netzwerklatenz aufgrund von IPSec. Verhandlungen.

> **Hinweis:** wenn Microsoft eine eigene Domänenisolierungslösung bereitgestellt hat, wurde die Nutzung im Netzwerk um ein bis drei Prozent als direkte Folge von IPSec erhöht.

Gruppenrichtlinien-Bereitstellungsgruppen und WMI-Filter

Sie müssen die Organisationseinheitshierarchie (OU) Ihrer Active Directory-Domänen nicht neu anordnen, um Windows Defender-Firewall-GPOs effektiv bereitzustellen. Stattdessen können Sie Ihre GPOs auf Domänenebene (oder einem anderen Container auf hoher Ebene) verknüpfen und dann mithilfe von Sicherheitsgruppenfilterung

oder WMI-Filterung sicherstellen, dass nur die entsprechenden Geräte oder Benutzer die GPO-Einstellungen anwenden können. Wir empfehlen, dass Sie die WMI-Filterung verwenden, um dynamisch zu gewährleisten, dass GPOs nur für Geräte gelten, die das richtige Betriebssystem ausführen. Sie müssen dieses Verfahren nicht verwenden, wenn Ihr Netzwerk aus Geräten besteht.

Verschiedene Active Directory-Vertrauens Umgebungen

Wenn Sie eine Domänen Isolierungs Richtlinie entwerfen, sollten Sie alle logischen Grenzen in Frage stellen, die sich möglicherweise auf IPsec-gesicherte Kommunikation auswirken. Beispielsweise sind die Vertrauensstellungen zwischen ihren Domänen und Gesamtstrukturen entscheidend für die Bestimmung einer geeigneten IKE-Authentifizierungsmethode.

Die KerberosV5-Authentifizierung wird für die Verwendung in einer bidirektionalen (gegenseitigen) Domänen- und Forest Trust-Umgebung empfohlen. Sie können KerberosV5 für die IKE-Authentifizierung in Domänen mit bidirektionalen Vertrauensstellungen verwenden, wenn sich die Domänen in derselben Gesamtstruktur oder in verschiedenen Gesamtstrukturen befinden. Wenn sich die beiden Domänen in unterschiedlichen Gesamtstrukturen befinden, müssen Sie zwei externe Vertrauensstellungen (eine für jede Richtung) zwischen den Domänen konfigurieren. Die externen Vertrauensstellungen müssen den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der Domänen verwenden, und die IPSec-Richtlinie muss es einem IKE-Initiator in einer Domäne ermöglichen, mit einem beliebigen Domänencontroller in der Gesamtstruktur-Domänenhierarchie zu kommunizieren, damit der Initiator ein KerberosV5-Ticket erhalten kann. von einem Domänencontroller in der Domäne des Responders. Wenn Firewalls die Domänen trennen, müssen Sie die Firewall so konfigurieren, dass KerberosV5-Datenverkehr über UDP-Zielport 88, TCP-Ziel-Port 88 und UDP-Ziel-Port 389 zulässig ist.

Wenn die Verwendung der KerberosV5-Authentifizierung nicht möglich ist, da bidirektionale Vertrauensstellungen über Gesamtstrukturen nicht wie in einigen größeren Unternehmensumgebungen eingerichtet werden können, können Sie eine Public Key-Infrastruktur (PKI) und digitale Zertifikate zum Einrichten von IPSec-vertrauenswürdigen Kommunikation.

Erstellen von Firewallregeln zum Zulassen von IKE-, AH-und ESP-Datenverkehr

In einigen Fällen muss der IPsec-gesicherte Datenverkehr möglicherweise durch einen Router, eine Umkreisfirewall oder ein anderes Filtergerät geleitet werden. Wenn der Router TCP-und UDP-Datenverkehr oder andere übergeordnete Protokoll Kopfzeilen nicht filtert, ist im Fall eines Routers keine spezielle Konfiguration erforderlich, damit der IPSec-Datenverkehr weitergeleitet werden kann.

Im Fall eines Filter Routers oder einer Firewall müssen Sie diese Geräte so konfigurieren, dass IPSec-Datenverkehr weitergeleitet werden kann. Konfigurieren Sie die Firewall so, dass IPSec-Datenverkehr für UDP-Quell-und Zielport 500 (IKE), UDP-Quell-und Ziel-Port 4500 (IPSec NAT-T) und IP-Protokoll 50 (ESP) zulässig ist. Möglicherweise müssen Sie auch die Firewall so konfigurieren, dass IPSec-Datenverkehr auf dem IP-Protokoll 51 (AH) die Problembehandlung durch IPSec-Administratoren zulässt und der IPSec-Datenverkehr überprüft werden kann.

Weitere Informationen finden Sie unter Aktivieren von IPSec-Datenverkehr über eine Firewall.

Netzwerklastenausgleich und Servercluster

Es bestehen Herausforderungen beim Implementieren der Verbindungssicherheit für den Netzwerkdatenverkehr, der zu und von Netzwerklastenausgleichs-Clustern und Serverclustern wird. Mithilfe von NLB können mehrere Server zusammen gruppiert werden, um eine höhere Verfügbarkeit für einen Dienst bereitzustellen, indem ein automatisches Failover auf andere Knoten im Cluster bereitgestellt wird. Da IPSec einer Sicherheitszuordnung zu einem bestimmten Gerät entspricht, wird verhindert, dass verschiedene Geräte dieselbe Clientverbindung

verarbeiten. Wenn ein anderer Knoten im Cluster auf eine IPSec-Verbindung antwortet, die ursprünglich von einem anderen Knoten eingerichtet wurde, wird der Datenverkehr vom Clientgerät als nicht vertrauenswürdig abgesetzt.

Das bedeutet, dass NLB im Modus "keine Affinität" überhaupt nicht von IPSec unterstützt wird. Wenn Sie den Modus "keine Affinität" im Cluster verwenden müssen, sollten Sie die Server, aus denen der Cluster besteht, in Ihre IPSec-Ausnahmegruppe einbeziehen und Clients die Kommunikation mit den Servern ohne IPSec ermöglichen.

Wenn eine TCP-Verbindung aufgrund eines Clusterknoten-Failovers abgebrochen wird, erkennt IPSec den TCP-Verbindungsfehler und entfernt die IPSec-SAS für diese Verbindung. Wenn die neue TCP-Verbindung zu einem anderen Knoten hergestellt wird, kann IPSec neue SAS sofort aushandeln, ohne auf eine Timeout Wartezeit für die veraltete SAS warten zu müssen.

Netzwerk inspektionstechnologien

Innerhalb eines TCP/IP-Pakets ändert IPSec ohne Verschlüsselung die Offsets für die Zielanschlüsse und-Protokolle. Diese Änderungen können sich negativ auf Anwendungen auswirken, die auf Netzwerkgeräten wie Routern ausgeführt werden, die den Datenverkehr im Netzwerk überwachen und verwalten. Während einige Netzwerkanwendungen zur Unterstützung von IPSec aktualisiert wurden, sind einige noch nicht kompatibel. Erkundigen Sie sich beim Hersteller Ihres Geräts, ob die von IPSec verursachten Änderungen in den Protokoll- und Port Feldern mit dem Gerät kompatibel sind.

Jedes Gerät, das zum Anzeigen des Netzwerkverkehrs entwickelt wurde, beispielsweise Hardwareprotokoll Analysatoren oder Microsoft-Netzwerk Monitor, kann keinen ESP-verschlüsselten Datenverkehr analysieren. Nur das Zielgerät, mit dem das ursprüngliche Gerät die Verbindung ausgehandelt hat, kann den Datenverkehr entschlüsseln.

Im allgemeinen besiegt IPSec die netzwerkbasierte Priorisierung und die Port-oder protokollbasierte Datenverkehrsverwaltung. Für verschlüsselte Pakete gibt es keine Problemumgehung. der Host selbst muss alle Datenverkehrs Verwaltungsfunktionen verarbeiten. Für unverschlüsselte, authentifizierte Pakete müssen sich die Geräte und Anwendungen bewusst sein, wie IPSec-Pakete geändert werden, damit Sie nichts anderes als die Weiterleitung an den richtigen Host tun können. Wenn Sie keine Überwachungs-oder Verwaltungsgeräte zur Unterstützung von IPSec aktualisieren können, ist es wichtig, dass Sie diese Informationen aufzeichnen und in Ihrem Domänen-oder Server Isolierungs Entwurf finden.

Der Netzwerk Monitor umfasst Parser für die Protokolle ISAKMP (IKE), AH und ESP. Netzwerk Monitor Parser für ESP können nur innerhalb des ESP-Pakets analysiert werden, wenn ESP-Null Verschlüsselung verwendet wird. Netzwerk Monitor kann die verschlüsselten Teile des IPSec-ESP-Datenverkehrs nicht analysieren, wenn die Verschlüsselung in der Software durchgeführt wird. Wenn die Verschlüsselung jedoch von einem Netzwerkadapter für die IPSec-Hardware Entlastung durchgeführt wird, können die ESP-Pakete entschlüsselt werden, wenn Sie vom Netzwerk Monitor entweder auf der Quelle oder im Ziel erfasst werden und daher analysiert werden können. Wenn Sie eine ESP-Software-verschlüsselte Kommunikation diagnostizieren möchten, müssen Sie die ESP-Verschlüsselung deaktivieren und die ESP-Null-Verschlüsselung verwenden, indem Sie die IPSec-Richtlinie oder die Verbindungssicherheitsregel auf beiden Geräten ändern.

Nachrichten Analyse steht im Microsoft Download Centerzur Verfügung.

Nächster Schritt: Ermitteln des vertrauenswürdigen Zustands Ihrer Geräte

Ermitteln des vertrauenswürdigen Zustands Ihrer Geräte

07.08.2019 • 9 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie Informationen zu den Geräten erhalten haben, die derzeit Teil der IT-Infrastruktur sind, müssen Sie ermitteln, zu welchem Zeitpunkt ein Gerät als vertrauenswürdig eingestuft wird. Der Begriff *Trusted* kann verschiedene Dinge für verschiedene Personen bedeuten. Daher müssen Sie für alle Projekt Beteiligten eine feste Definition für das Projekt übermitteln. Wenn dies nicht der Fall ist, kann dies zu Problemen mit der Sicherheit der vertrauenswürdigen Umgebung führen, da die Gesamtsicherheit nicht die Sicherheitsstufe überschreiten kann, die vom am wenigsten sicheren Client festgesetzt wird, der den vertrauenswürdigen Status erreicht.

> **Hinweis:** in diesem Kontext hat der Begriff *Trust* nichts mit einer Active Directory-Vertrauensstellung zwischen Domänen zu tun. Der vertrauenswürdige Zustand Ihrer Geräte zeigt nur den Grad des Risikos an, den Sie glauben, dass das Gerät in das Netzwerk einführt. Vertrauenswürdige Geräte bringen kaum Risiken mit sich, während nicht vertrauenswürdige Geräte potenziell zu großem Risiko führen können.

Vertrauens Zustände

Um dieses Konzept zu verstehen, sollten Sie die vier grundlegenden Zustände beachten, die für Geräte in einer typischen IT-Infrastruktur gelten. Diese Zustände sind (in der Reihenfolge des Risikos zuerst das niedrigste Risiko):

- Vertrauenswürdigen
- Vertrauenswürdigkeit
- Bekannt, nicht vertrauenswürdig
- Unbekannt, nicht vertrauenswürdig

Im Rest dieses Abschnitts werden diese Zustände definiert, und Sie erfahren, wie Sie feststellen können, welche Geräte in Ihrer Organisation zu den einzelnen Zuständen gehören.

Vertrauenswürdiger Zustand

Wenn Sie ein Gerät als vertrauenswürdig einstufen, bedeutet dies, dass die Sicherheitsrisiken des Geräts verwaltet werden, was jedoch nicht bedeutet, dass es vollkommen sicher oder unverwundbar ist. Die Verantwortung für diesen verwalteten Zustand fällt den IT-und Sicherheitsadministratoren zusätzlich zu den Benutzern, die für die Konfiguration des Geräts verantwortlich sind. Ein vertrauenswürdiges Gerät, das schlecht verwaltet wird, wird wahrscheinlich zu einem Schwachpunkt für das Netzwerk.

Wenn ein Gerät als vertrauenswürdig eingestuft wird, können andere vertrauenswürdige Geräte davon ausgehen, dass das Gerät keinen böswilligen Akt initiiert. Vertrauenswürdige Geräte können beispielsweise davon ausgehen, dass andere vertrauenswürdige Geräte keinen Virus ausführen, der Sie angreift, da alle vertrauenswürdigen Geräte Mechanismen (wie Antivirensoftware) verwenden müssen, um die Bedrohung durch Viren zu minimieren.

Verbringen Sie einige Zeit damit, die Ziele und Technologieanforderungen zu definieren, die Ihre Organisation als die Mindestkonfiguration für ein Gerät für den vertrauenswürdigen Status erachtet.

Eine mögliche Liste der Technologieanforderungen kann Folgendes umfassen:

- **Betriebssystem.** Ein vertrauenswürdiges Clientgerät sollte mindestens Windows Vista ausgeführt werden. Auf einem vertrauenswürdigen Server sollte mindestens Windows Server2008 ausgeführt werden.
- **Domänenmitgliedschaft.** Ein vertrauenswürdiges Gerät gehört zu einer verwalteten Active Directory-Domäne, was bedeutet, dass die IT-Abteilung über Sicherheits Verwaltungsrechte verfügt und Mitglieds Geräte mithilfe von Gruppenrichtlinien konfigurieren kann.
- **Verwaltungsclient.** Alle vertrauenswürdigen Geräte müssen einen bestimmten Netzwerk Verwaltungsclient ausführen, um eine zentralisierte Verwaltung und Steuerung von Sicherheitsrichtlinien, Konfigurationen und Software zu ermöglichen. Configuration Manager ist ein solches Verwaltungssystem mit einem geeigneten Client.
- **Antivirus-Software.** Alle vertrauenswürdigen Geräte führen Antivirensoftware aus, die so konfiguriert ist, dass die neuesten Virussignaturdateien täglich überprüft und automatisch aktualisiert werden.
- **Dateisystem.** Alle vertrauenswürdigen Geräte werden für die Verwendung des NTFS-Dateisystems konfiguriert.
- **BIOS-Einstellungen.** Alle vertrauenswürdigen tragbaren Geräte werden so konfiguriert, dass Sie ein Kennwort auf BIOS-Ebene verwenden, das der Verwaltung des IT-Support Teams unterliegt.
- **Kennwortanforderungen** Vertrauenswürdige Clients müssen sichere Kennwörter verwenden.

Es ist wichtig zu verstehen, dass der vertrauenswürdige Zustand nicht konstant ist; Hierbei handelt es sich um einen vorübergehenden Zustand, der sich ändernde Sicherheitsstandards und die Einhaltung dieser Standards unterliegt. Neue Bedrohungen und neue Verteidigungsanlagen entstehen ständig. Aus diesem Grund müssen die Verwaltungssysteme des Unternehmens die vertrauenswürdigen Geräte kontinuierlich überprüfen, um die laufende Compliance zu gewährleisten. Darüber hinaus müssen die Verwaltungssysteme in der Lage sein, Updates oder Konfigurationsänderungen auszugeben, wenn diese erforderlich sind, um den vertrauenswürdigen Status zu gewährleisten.

Ein Gerät, das alle diese Sicherheitsanforderungen weiterhin erfüllt, kann als vertrauenswürdig eingestuft werden. Es ist jedoch möglich, dass die meisten Geräte, die in dem zuvor besprochenen Ermittlungsprozess identifiziert wurden, diese Voraussetzungen nicht erfüllen. Sie müssen daher angeben, welche Geräte vertrauenswürdig sind und welche nicht. Zur Unterstützung dieses Prozesses verwenden Sie den *vertrauenswürdigen* Zwischenzustand. Im weiteren Verlauf dieses Abschnitts werden die verschiedenen Zustände und ihre Auswirkungen erläutert.

Vertrauenswürdiger Zustand

Es ist hilfreich, so schnell wie möglich die Geräte in der aktuellen Infrastruktur zu identifizieren, die einen vertrauenswürdigen Zustand erreichen können. Ein *vertrauenswürdiger Zustand* kann zugewiesen werden, um anzugeben, dass das aktuelle Gerät den vertrauenswürdigen Zustand mit den erforderlichen Software-und Konfigurationsänderungen physisch erreichen kann.

Erstellen Sie für jedes Gerät, dem ein vertrauenswürdiger Status zugewiesen ist, eine zugehörige Konfigurations Notiz, in der angegeben ist, was erforderlich ist, damit das Gerät den vertrauenswürdigen Status erhält. Diese Informationen sind für das Projekt Design Team besonders wichtig (um die Kosten für das Hinzufügen des Geräts zur Lösung zu schätzen) und die Mitarbeiter des Supports (um Ihnen die Anwendung der erforderlichen Konfiguration zu ermöglichen).

Im allgemeinen fallen vertrauenswürdige Geräte in eine der folgenden beiden Gruppen:

- **Konfiguration erforderlich.** Mit der aktuellen Hardware, dem Betriebssystem und der Software kann das Gerät einen vertrauenswürdigen Zustand erreichen. Es sind jedoch zusätzliche Konfigurationsänderungen erforderlich. Wenn die Organisation beispielsweise ein sicheres Dateisystem erfordert, bevor ein Gerät als vertrauenswürdig eingestuft werden kann, erfüllt ein Gerät, das eine FAT32-formatierte Festplatte

verwendet, diese Anforderung nicht.

- **Upgrade erforderlich.** Diese Geräte erfordern Upgrades, bevor Sie als vertrauenswürdig eingestuft werden können. Die folgende Liste enthält einige Beispiele für die Art des Upgrades, die für diese Geräte möglicherweise erforderlich sind:
  - **Upgrade des Betriebssystems erforderlich.** Wenn das aktuelle Betriebssystem des Geräts die Sicherheitsanforderungen der Organisation nicht unterstützenkann, wäre ein Upgrade erforderlich, bevor das Gerät einen vertrauenswürdigen Zustand erreichen kann.
  - **Software erforderlich.** Ein Gerät, das eine erforderliche Sicherheitsanwendung, beispielsweise einen Antivirus-Scanner oder einen Verwaltungsclient, fehlt, kann erst dann als vertrauenswürdig eingestuft werden, wenn diese Anwendungen installiert und aktiv sind.
  - **Hardware-Upgrade erforderlich.** In einigen Fällen ist für ein Gerät möglicherweise ein bestimmtes Hardware Upgrade erforderlich, bevor der vertrauenswürdige Status erreicht werden kann. Dieser Gerätetyp benötigt in der Regel ein Upgrade des Betriebssystems oder zusätzliche Software, die das erforderliche Hardware-Upgrade erzwingt. Beispielsweise kann für Sicherheitssoftware zusätzlicher Festplattenspeicher auf dem Gerät erforderlich sein.
  - **Geräteaustausch erforderlich.** Diese Kategorie ist für Geräte reserviert, die die Sicherheitsanforderungen der Lösung nicht unterstützen können, da Ihre Hardware die minimale akzeptable Konfiguration nicht unterstützenkann. Beispielsweise ein Gerät, auf dem kein sicheres Betriebssystem ausgeführt werden kann, da es über einen alten Prozessor verfügt (wie etwa ein auf x86 basierendes Gerät mit 100 MHz).

Verwenden Sie diese Gruppen, um die Kosten für die Implementierung der Lösung auf den Geräten, die Upgrades erfordern, zuzuweisen.

Bekannter, nicht vertrauenswürdiger Zustand

Während der Kategorisierung der Geräte einer Organisation werden Sie einige Geräte identifizieren, die für bestimmte, gut verständliche und klar definierte Gründe keinen vertrauenswürdigen Status erreichen können. Diese Gründe können die folgenden Typen enthalten:

- **Finanz.** Die Finanzierung steht nicht zur Verfügung, um die Hardware oder Software für dieses Gerät zu aktualisieren.
- **Politischen.** Das Gerät muss aufgrund einer politischen oder geschäftlichen Situation in einem nicht vertrauenswürdigen Zustand verbleiben, das es nicht in der Lage ist, die angegebenen Mindestsicherheits Anforderungen der Organisation zu erfüllen. Es wird dringend empfohlen, dass Sie sich an den Unternehmensbesitzer oder den unabhängigen Softwarehersteller (Independent Software Vendor, ISV) für das Gerät wenden, um den Mehrwert der Server-und Domänenisolierung zu besprechen.
- **Funktions.** Auf dem Gerät muss ein nicht sicheres Betriebssystem ausgeführt werden, oder es muss auf unsichere Weise funktionieren, um seine Rolle zu erfüllen. Beispielsweise kann es erforderlich sein, dass das Gerät ein älteres Betriebssystem ausführt, da eine bestimmte Branchenanwendung nur für dieses Betriebssystem verwendet werden kann.

Es kann mehrere Funktions Gründe geben, damit ein Gerät im bekannten nicht vertrauenswürdigen Zustand verbleibt. Die folgende Liste enthält mehrere Beispiele für funktionelle Gründe, die zu einer Klassifizierung dieses Zustands führen können:

- **Geräte, auf denen nicht unterstützte Windows-Versionen ausgeführt werden.** Dazu gehören Windows XP, Windows MillenniumEdition, Windows98, Windows95 oder WindowsNT. Geräte, auf denen diese Versionen des Windows-Betriebssystems ausgeführt werden, können nicht als vertrauenswürdig eingestuft werden, da diese Betriebssysteme die erforderliche Sicherheitsinfrastruktur nicht unterstützen. Obwohl WindowsNT eine grundlegende Sicherheitsinfrastruktur unterstützt, unterstützt Sie beispielsweise

keine "Deny"-ACLs für lokale Ressourcen, um die Vertraulichkeit und Integrität der Netzwerkkommunikation, Smartcards für eine starke Authentifizierung zu gewährleisten, oder zentralisierte Verwaltung von Gerätekonfigurationen (obwohl eine begrenzte zentrale Verwaltung von Benutzerkonfigurationen unterstützt wird).

- **Eigenständige Geräte.** Geräte, auf denen eine beliebige Version von Windows ausgeführt wird, die als eigenständige Geräte oder als Mitglieder einer Arbeitsgruppe konfiguriert sind, können in der Regel keinen vertrauenswürdigen Zustand erreichen. Obwohl diese Geräte die Mindestanforderungen für die grundlegende Sicherheitsinfrastruktur vollständig unterstützen, sind die erforderlichen Sicherheitsverwaltungsfunktionen wahrscheinlich nicht verfügbar, wenn das Gerät nicht Bestandteileiner vertrauenswürdigen Domäne ist.
- **Geräte in einer nicht vertrauenswürdigen Domäne.** Ein Gerät, das Mitglied einer Domäne ist, die von der IT-Abteilung einer Organisation nicht als vertrauenswürdig eingestuft wird, kann nicht als vertrauenswürdig eingestuft werden. Bei einer nicht vertrauenswürdigen Domäne handelt es sich um eine Domäne, die die erforderlichen Sicherheitsfunktionen für ihre Mitglieder nicht bereitstellen kann. Obwohl die Betriebssysteme von Geräten, die Mitglieder dieser nicht vertrauenswürdigen Domäne sind, möglicherweise die Mindestanforderungen für die grundlegende Sicherheitsinfrastruktur vollständig unterstützen, können die erforderlichen Sicherheitsverwaltungsfunktionen nicht vollständig gewährleistet werden, wenn sich die Geräte nicht in einem vertrauenswürdigen Domäne.

Unbekannter, nicht vertrauenswürdiger Zustand

Der unbekannte, nicht vertrauenswürdige Zustand sollte als Standardzustand für alle Geräte angesehen werden. Da Geräte in diesem Zustand über eine unbekannte Konfiguration verfügen, können Sie Ihnen keine Vertrauensstellung zuweisen. Bei der Planung für Geräte in diesem Zustand muss davon ausgegangen werden, dass das Gerät ein nicht akzeptables Risiko für die Organisation darstellt. Designer der Lösung sollten sich bemühen, die Auswirkungen zu minimieren, die die Geräte in diesem Zustand auf ihre Organisationen haben können.

Aufzeichnen von Aktualisierungskosten für aktuelle Geräte

Der letzte Schritt in diesem Teil des Prozesses besteht darin, die ungefähren Kosten für das Upgrade der Geräte auf einen Punkt aufzuzeichnen, an dem Sie am Server-und Domänen Isolierungs Entwurf teilnehmen können. Sie müssen in der Entwurfsphase des Projekts mehrere wichtige Entscheidungen treffen, die Antworten auf die folgenden Fragen erfordern:

- Erfüllt das Gerät die für die Isolierung erforderlichen Hardwarevoraussetzungen?
- Erfüllt das Gerät die für die Isolierung erforderlichen Mindestvoraussetzungen für Software?
- Welche Konfigurationsänderungen müssen vorgenommen werden, um dieses Gerät in die Isolierungslösung zu integrieren?
- Was sind die voraussichtlichen Kosten oder Auswirkungen der vorgeschlagenen Änderungen, damit das Gerät einen vertrauenswürdigen Zustand erhält?

Durch die Beantwortung dieser Fragen können Sie schnell ermitteln, wie hoch der Aufwand und die ungefähren Kosten sind, mit denen ein bestimmtes Gerät oder eine bestimmte Gruppe von Geräten in den Projektumfang gebracht wird. Beachten Sie, dass der Zustand eines Geräts transitiv ist und dass Sie durch Ausführen der aufgelisteten Abhilfe Aktionen den Zustand eines Geräts von "nicht vertrauenswürdig" auf "vertrauenswürdig" ändern können. Nachdem Sie entschieden haben, ob ein Gerät in einem vertrauenswürdigen Zustand platziert werden soll, können Sie mit dem Planen und Entwerfen der Isolierungsgruppen beginnen, die im nächsten Abschnitt Planen von Domänen Isolations Zonen erläutert werden.

In der folgenden Tabelle finden Sie ein Beispiel für ein Datenblätter Verzeichnis, das Sie beim Erfassen des aktuellen Zustands eines Geräts verwenden können, und was für das Gerät erforderlich ist, um einen

vertrauenswürdigen Zustand zu erreichen.

GERÄTENAME	HARDWARE-REQS ERFÜLLT	SOFTWARE-REQS ERFÜLLT	KONFIGURATION ERFORDERLICH	DETAILS	GEPLANTE KOSTEN
CLIENT001	Nein	Nein	Aktualisieren von Hardware und Software.	Das aktuelle Betriebssystem ist WindowsXP. Alte Hardware ist mit neueren Versionen von Windows nicht kompatibel.	$??
SERVER001	Ja	Nein.	Teilnehmen an einer vertrauenswürdigen Domäne und Upgrade von Windows Server 2003 auf Windows Server 2012.	Keine Antivirus-Software vorhanden.	$??

In der vorhergehenden Tabelle ist die Geräte-CLIENT001 derzeit "bekannt, nicht vertrauenswürdig", da Ihre Hardware aktualisiert werden muss. Es kann jedoch als vertrauenswürdig eingestuft werden, wenn die erforderlichen Upgrades möglich sind. Wenn jedoch für viele Geräte dieselben Upgrades erforderlich sind, sind die Gesamtkosten der Lösung deutlich höher.

Das Geräte-SERVER001 ist "vertrauenswürdig", da es die Hardwareanforderungen erfüllt, das Betriebssystem aber aktualisiert werden muss. Außerdem ist eine Antivirus-Software erforderlich. Bei den voraussichtlichen Kosten handelt es sich um die Menge an Aufwand, die erforderlich ist, um das Betriebssystem zu aktualisieren und die Antivirensoftware sowie deren Anschaffungskosten zu installieren.

Mit den anderen Informationen, die Sie in diesem Abschnitt gesammelt haben, sind diese Informationen die Grundlage für die Bemühungen, die später im Abschnitt Planen von Domänen Isolations Zonen durchgeführt wurden.

Die in diesem Abschnitt angegebenen Kosten erfassen nur die voraussichtlichen Kosten für die Geräte Upgrades. Viele zusätzliche Design-, Support-, Test-und Schulungskosten sollten im Gesamtprojektplan berücksichtigt werden.

Nächster Schritt: Planen der Windows Defender-Firewall mit erweitertem Sicherheits Design

Planen der Windows Defender-Firewall mit erweitertem Sicherheits Design

07.08.2019 • 4 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie die relevanten Informationen in den vorherigen Abschnitten gesammelt und die Grundlagen der Entwürfe verstanden haben, wie weiter oben in diesem Leitfaden beschrieben, können Sie das Design (oder die Kombination von Designs) auswählen, das Ihren Anforderungen entspricht.

Grundlegender Firewall-Entwurf

Wir empfehlen, mindestens das grundlegende Firewall-Design bereitzustellen. Wie im Abschnitt Schützen von Geräten vor unerwünschtem Netzwerkverkehr erläutert, sind hostbasierte Firewalls ein wichtiges Element in einer umfassenden Verteidigungsstrategie und ergänzen die meisten anderen Sicherheitsmaßnahmen, die Sie in Ihrer Organisation durchgeführt haben.

Wenn Sie bereit sind, die Optionen für Firewall-Richtlinieneinstellungen zu überprüfen, lesen Sie den Abschnitt Planungseinstellungen für eine grundlegende Firewall-Richtlinie .

Unterstützung und Auswahl von Algorithmen und Methoden

Wenn Sie eine Domänenisolierung oder einen Server Isolierungs Entwurf erstellen möchten, müssen Sie die in jeder Windows-Version verfügbaren Algorithmen sowie ihre relativen Stärken verstehen.

Überlegungen zur IPSec-Leistung

Obwohl IPSec für die Sicherung des Netzwerkdatenverkehrs von und zu Ihren Geräten von entscheidender Bedeutung ist, gibt es Kosten, die mit der Verwendung verbunden sind. Die mathematisch intensiven kryptografischen Algorithmen erfordern eine beträchtliche Menge an Rechenleistung, wodurch verhindert wird, dass Ihr Gerät alle verfügbare Bandbreite nutzen kann. Beispielsweise kann ein IPSec-fähiges Gerät, das die AES-Verschlüsselungsprotokolle auf einem Netzwerk Link mit 10 Gigabit pro Sekunde (Gbit/s) verwendet, einen Durchsatz von 4,5 Gbit/s sehen. Dies liegt an den Anforderungen an die CPU, um die kryptografischen Funktionen auszuführen, die für die IPSec-Integritäts-und Verschlüsselungsalgorithmen erforderlich sind.

IPSec-Aufgaben Entlastung ist eine Windows-Technologie, die Netzwerkadapter unterstützt, die mit dedizierten kryptografischen Prozessoren ausgestattet sind, um die von IPSec benötigte rechenintensive Arbeit durchzuführen. Dadurch wird die CPU eines Geräts freigegeben, und der Netzwerkdurchsatz kann drastisch erhöht werden. Für denselben Netzwerk Link wie oben wird der Durchsatz mit aktivierter IPSec-Aufgaben Entlastung auf etwa 9,2 Gbit/s verbessert.

Design der Domänenisolierung

Dieses Design in ihre Pläne einbeziehen:

- Wenn Sie über eine Active Directory-Domäne verfügen, von der die meisten Geräte Mitglieder sind.
- Wenn Sie verhindern möchten, dass die Geräte in Ihrer Organisation unerwünschten

Netzwerkdatenverkehr von Geräten akzeptieren, die nicht Teil der Domäne sind.

Wenn Sie das grundlegende Firewall-Design als Teil Ihrer Bereitstellung einbeziehen möchten, sollten Sie zuerst die Firewall-Richtlinien bereitstellen, um zu bestätigen, dass Sie ordnungsgemäß funktionieren. Planen Sie auch, die Verbindungssicherheitsregeln zunächst im Anforderungsmodus zu aktivieren, anstatt den restriktiveren require-Modus zu verwenden, bis Sie sicher sind, dass alle Geräte den Netzwerkverkehr mit IPSec ordnungsgemäß schützen. Wenn etwas nicht stimmt, ermöglicht der Anforderungsmodus weiterhin, dass die Kommunikation fortgesetzt wird, während Sie die Problembehandlung durchführen.

Wenn Sie bereit sind, die Optionen zum Erstellen einer isolierten Domäne zu überprüfen, lesen Sie den Abschnitt Planning Domain Isolation Zones .

Server Isolierungs Entwurf

Dieses Design in ihre Pläne einbeziehen:

- Wenn Sie über eine isolierte Domäne verfügen und den Zugriff auf bestimmte Server zusätzlich auf autorisierte Benutzer und Geräte einschränken möchten.
- Sie stellen keine isolierte Domäne bereit, möchten aber ähnliche Vorteile für einige bestimmte Server nutzen. Sie können den Zugriff auf die isolierten Server nur auf autorisierte Benutzer und Geräte einschränken.

Wenn Sie eine Domänenisolierung in Ihre Bereitstellung einbeziehen möchten, empfiehlt es sich, diesen Layer abzuschließen und den korrekten Vorgang zu bestätigen, bevor Sie die zusätzlichen Server Isolations Elemente implementieren.

Wenn Sie bereit sind, die Optionen zum Isolieren von Servern zu untersuchen, lesen Sie den Abschnitt Planning Server-Isolierungs Zonen .

Zertifikatbasiertes Authentifizierungs Design

Dieses Design in ihre Pläne einbeziehen:

- Wenn Sie einige der Elemente der Domänen-oder Serverisolierung auf Geräten implementieren möchten, die nicht mit einer Active Directory-Domäne verbunden sind, oder wenn Sie die Domänenmitgliedschaft nicht als Authentifizierungsmechanismus verwenden möchten.
- Sie verfügen über eine isolierte Domäne und möchten einen Server einbeziehen, der kein Mitglied der Active Directory-Domäne ist, da auf dem Gerät nicht Windows ausgeführt wird, oder aus einem anderen Grund.
- Sie müssen externe Geräte aktivieren, die nicht von Ihrer Organisation verwaltet werden, um auf Informationen auf einem Ihrer Server zuzugreifen, und möchten dies auf sichere Weise tun.

Wenn Sie beabsichtigen, eine Domänen-oder Serverisolierung in Ihre Bereitstellung einzubeziehen, empfehlen wir, diese Elemente zu vervollständigen und deren korrekten Betrieb zu bestätigen, bevor Sie die zertifikatbasierte Authentifizierung den Geräten hinzufügen, die Sie benötigen.

Wenn Sie bereit sind, die Optionen für die Verwendung der zertifikatbasierten Authentifizierung zu untersuchen, lesen Sie den Abschnitt Planen der zertifikatbasierten Authentifizierung .

Dokumentieren Ihres Entwurfs

Nachdem Sie die Auswahl der verwendeten Designs abgeschlossen haben, müssen Sie die einzelnen Geräte der entsprechenden Isolierungs Zone zuweisen und die Aufgabe für die Verwendung durch das Bereitstellungsteam dokumentieren.

- Dokumentieren der Zonen

Entwerfen von Gruppen und GPOs

Nachdem Sie ein Design ausgewählt und Ihre Geräte Zonen zugewiesen haben, können Sie mit dem Festlegen der Isolierungsgruppen für jede Zone, den Netzwerkzugriffsgruppen für den Zugriff auf den isolierten Server und den GPOs beginnen, die Sie verwenden, um die Einstellungen und Regeln auf Ihre Geräte anzuwenden.

Wenn Sie bereit sind, die Optionen für die Gruppen, Filter und GPOs zu untersuchen, lesen Sie den Abschnitt Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen .

Nächster Schritt: Planungseinstellungen für eine grundlegende Firewall-Richtlinie

Planen der Einstellungen für eine allgemeine Firewallrichtlinie

07.08.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie Ihre Anforderungen identifiziert und die Informationen über das Netzwerklayout und die verfügbaren Geräte bereitgestellt haben, können Sie mit dem Entwerfen der GPO-Einstellungen und-Regeln beginnen, die es Ihnen ermöglichen, Ihre Anforderungen auf den Geräten durchzusetzen.

Im folgenden finden Sie eine Liste der Firewalleinstellungen, die Sie möglicherweise für die Aufnahme in ein einfaches Firewall-Design in Frage stellen, sowie Empfehlungen, die als Ausgangspunkt für Ihre Analyse dienen:

- **Profilauswahl**. Die Firewallregeln können für alle Netzwerkstandort Profile konfiguriert werden, die im Netzwerk-und Freigabe Center angezeigt werden: **Domäne**, **öffentlich**und **Privat**. Die meisten Einstellungen werden im Domänenprofil erzwungen, ohne dass der Benutzer die Möglichkeit hat, Sie zu ändern. Möglicherweise möchten Sie jedoch die vom benutzerkonfigurierbaren Profileinstellungen auf Geräten belassen, die vom physikalischen Netzwerk der Organisation übernommen und mit einem öffentlichen oder privaten Netzwerk verbunden werden können. Wenn Sie die öffentlichen und privaten profile sperren, können Sie verhindern, dass ein Benutzer auf ein erforderliches Netzwerkprogramm oder einen erforderlichen Dienst zugreift. Da Sie sich nicht im Netzwerk der Organisation befinden, können Sie kein Verbindungsproblem beheben, indem Sie Regeländerungen in einem Gruppenrichtlinienobjekt bereitstellen. Beachten Sie für jeden der folgenden Abschnitte jedes Profil, und wenden Sie die Regeln auf die Profile an, die für Ihre Organisation sinnvoll sind.

  > **Wichtig:** es wird empfohlen, dass Sie auf Server Geräten alle Regeln für alle Profile fest legen, um zu verhindern, dass unerwartete Profilwechsel die Netzwerkkonnektivität stören. Sie können eine ähnliche Vorgehensweise für Ihre Desktop Geräte in Frage stellen und nur unterschiedliche Profile auf tragbaren Geräten unterstützen.

- **Firewall-Status: ein**. Wir empfehlen, dass Sie den Benutzer daran hindern, ihn auszuschalten.
- **Standardverhalten für eingehende Verbindungen: Block**. Wir empfehlen, das Standardverhalten für das Blockieren von unerwünschten eingehenden Verbindungen zu erzwingen. Wenn Sie Netzwerkdatenverkehr für ein bestimmtes Programm zulassen möchten, erstellen Sie eine eingehende Regel, die als Ausnahme für dieses Standardverhalten dient.
- **Standardverhalten für ausgehende Verbindungen: zulassen**. Wir empfehlen, dass Sie das Standardverhalten erzwingen, wenn ausgehende Verbindungen zugelassen werden.
- **Unicast-Antwort zulassen: Ja**. Wir empfehlen, dass Sie die Standardeinstellung " **Ja** " verwenden, es sei denn, Sie haben bestimmte Anforderungen, die ansonsten zu erfüllen sind.
- **Anwenden lokaler Firewallregeln: Ja**. Wir empfehlen, dass Sie Benutzern das Erstellen und Verwenden von lokalen Firewallregeln gestatten. Wenn Sie auf **Nein**klicken, wenn ein Benutzer auf **zulassen** auf die Benachrichtigung klickt, um den Datenverkehr für ein neues Programm zuzulassen, wird von Windows keine neue Firewallregel erstellt, und der Datenverkehr bleibt blockiert.

Wenn Sie und die IT-Mitarbeiter die Liste der Firewallregeln für alle zulässigen Anwendungen erstellen und verwalten können und diese mithilfe von GPOs bereitstellen, können Sie diesen Wert auf **Nein**einstellen.

- **Anwenden von Regeln für die lokale Verbindungssicherheit: Nein**. Wir empfehlen, dass Sie verhindern, dass Benutzer eigene Verbindungssicherheitsregeln erstellen und verwenden. Verbindungsfehler, die durch in Konflikt stehende Regeln verursacht werden, können schwer zu beheben sein.

- **Protokollierung**. Wir empfehlen, die Protokollierung in einer Datei auf der lokalen Festplatte zu aktivieren. Achten Sie darauf, die Größe zu begrenzen, beispielsweise 4096KB, um Leistungsprobleme zu vermeiden, indem Sie die Festplatte des Benutzers ausfüllen. Stellen Sie sicher, dass Sie einen Ordner angeben, in dem das Windows Defender-Firewall mit dem erweiterten Sicherheitsdienst Konto über Schreibberechtigungen verfügt.

- **Eingehende Regeln**. Erstellen Sie eingehende Regeln für Programme, die unerwünschte eingehende Netzwerkpakete von einem anderen Gerät im Netzwerk empfangen können. Machen Sie die Regeln so spezifisch wie möglich, um das Risiko schädlicher Programme, die die Regeln ausnutzen, zu verringern. Geben Sie beispielsweise sowohl Programm-als auch Portnummern an. Durch die Angabe eines Programms wird sichergestellt, dass die Regel nur aktiv ist, wenn das Programm tatsächlich ausgeführt wird, und durch Angabe der Portnummer wird sichergestellt, dass das Programm keinen unerwarteten Datenverkehr an einem anderen Port empfangen kann.

  Eingehende Regeln sind auf Servern üblich, da Sie Dienste hosten, mit denen Clientgeräte eine Verbindung herstellen. Wenn Sie Programme und Dienste auf einem Server installieren, erstellt und aktiviert das Installationsprogramm normalerweise die Regeln für Sie. Überprüfen Sie die Regeln, um sicherzustellen, dass Sie nicht mehr Ports als erforderlich öffnen.

  > **Wichtig:** Wenn Sie eingehende Regeln erstellen, die RPC-Netzwerkdatenverkehr mithilfe der Optionen für **RPC-Endpunktzuordnung** und **dynamische RPC** -Regel zulassen, ist der gesamte eingehende RPC-Netzwerkdatenverkehr zulässig, weil die Firewall das Netzwerk nicht filtern kann. Datenverkehr basierend auf der UUID der Zielanwendung.

- **Ausgehende Regeln**. Erstellen Sie nur ausgehende Regeln zum Blockieren des Netzwerkverkehrs, die in allen Fällen verhindert werden müssen. Wenn Ihre Organisation die Verwendung bestimmter Netzwerkprogramme verbietet, können Sie diese Richtlinie unterstützen, indem Sie den bekannten Netzwerkdatenverkehr blockieren, der vom Programm verwendet wird. Testen Sie unbedingt die Einschränkungen, bevor Sie Sie bereitstellen, um zu verhindern, dass der Datenverkehr für erforderliche und autorisierte Programme gestört wird.

Nächster Schritt: Planen von Domänen Isolierungs Zonen

Planen von Domänenisolationszonen

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie über die erforderlichen Informationen zu Ihrem Netzwerk, zu Active Directory sowie zu Client-und Server Geräten verfügen, können Sie diese Informationen verwenden, um Entscheidungen über die Isolierungs Zonen zu treffen, die Sie in Ihrer Umgebung verwenden möchten.

Der Großteil der Arbeit in Planning Server und Domänenisolierung bestimmt, welche Geräte jeder Isolierungs Zone zugewiesen werden sollen. Die ordnungsgemäße Auswahl der Zone für jedes Gerät ist wichtig für die Bereitstellung der richtigen Sicherheitsstufe, ohne die Leistung zu beeinträchtigen oder die Möglichkeit für ein Gerät zum Senden oder empfangen des erforderlichen Netzwerkverkehrs zu schaffen.

Zu den in diesem Leitfaden beschriebenen Zonen gehören die folgenden:

- Ausnahmeliste
- Isolierte Domäne
- Begrenzungszone
- Verschlüsselungszone

Ausnahmeliste

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie ein Sicherheitsmodell für Server und Domänenisolierung in Ihrer Organisation implementieren, finden Sie wahrscheinlich einige zusätzliche Herausforderungen. Wichtige Infrastrukturserver wie DNS-Server und DHCP-Server müssen in der Regel für alle Geräte auf dem internen Netzwerk zur Verfügung stehen, die jedoch vor Netzwerkangriffen geschützt sind. Wenn Sie jedoch für alle Geräte im Netzwerk, nicht nur für isolierte Domänenmitglieder, verfügbar sein müssen, können diese Server keine IPSec für den eingehenden Zugriff erfordern und auch nicht den IPSec-Transportmodus für ausgehenden Datenverkehr verwenden.

Zusätzlich zu den oben erwähnten Infrastrukturservern gibt es möglicherweise auch andere Server im Netzwerk, für die vertrauenswürdige Geräte nicht IPSec für den Zugriff verwenden können, die der Ausnahmeliste hinzugefügt werden.

Im Allgemeinen sind die folgenden Bedingungen Gründe für das Hinzufügen eines Geräts zur Ausnahmeliste:

- Wenn auf das Gerät von vertrauenswürdigen Geräten zugegriffen werden muss, aber keine kompatible IPSec-Implementierung.
- Wenn das Gerät Dienste für vertrauenswürdige und nicht vertrauenswürdige Geräte bereitstellen muss, aber die Kriterien für die Mitgliedschaft in der Grenz Zone nicht erfüllt.
- Wenn auf das Gerät von vertrauenswürdigen Geräten aus unterschiedlichen isolierten Domänen zugegriffen werden muss, für die keine Active Directory-Vertrauensstellung zueinander besteht.
- Wenn es sich bei dem Gerät um einen Domänencontroller mit einer älteren Windows-Version als Windows-Server2008 handelt oder wenn auf einem seiner Clients eine Version von Windows vor Windows Vista ausgeführt wird.
- Wenn das Gerät vertrauenswürdige und nicht vertrauenswürdige Geräte unterstützen muss, aber IPSec nicht verwenden kann, um die Kommunikation zu vertrauenswürdigen Geräten zu schützen.

Bei großen Organisationen kann die Liste der Ausnahmen sehr groß werden, wenn alle Ausnahmen durch eine Verbindungssicherheitsregel für die gesamte Domäne oder für alle vertrauenswürdigen Gesamtstrukturen implementiert werden. Wenn Sie festlegen können, dass alle Geräte in ihrer isolierten Domäne mindestens Windows Vista oder Windows Server2008 ausführen können, können Sie die Größe dieser Liste erheblich verkleinern. Eine große Ausnahmeliste hat mehrere unerwünschte Auswirkungen auf jedes Gerät, das das Gruppenrichtlinienobjekt empfängt, einschließlich der folgenden:

- Verringert die Gesamteffektivität der Isolierung.
- Verursacht eine größere Verwaltungsbelastung (aufgrund häufiger Updates).
- Vergrößert die IPSec-Richtlinie, was bedeutet, dass Sie mehr Arbeitsspeicher und CPU-Ressourcen beansprucht, den Netzwerkdurchsatz verlangsamt und die erforderliche Zeit zum herunterladen und Anwenden des Gruppenrichtlinienobjekts mit der IPSec-Richtlinie verlängert.

Um die Anzahl der Ausnahmen so klein wie möglich zu halten, gibt es mehrere Möglichkeiten:

- Berücksichtigen Sie die Kommunikationsanforderungen jeder Isolierungs Zone, insbesondere Server

Zonen, sorgfältig. Sie müssen möglicherweise nicht mit jeder Ausnahme in der Richtlinie auf Domänenebene für Clients kommunizieren.

- Konsolidieren von Serverfunktionen Wenn mehrere ausgeschlossene Dienste unter einer IP-Adresse gehostet werden können, wird die Anzahl der Ausnahmen verringert.
- Konsolidieren Sie ausgeschlossene Hosts im gleichen Subnetz. Wenn Netzwerkdatenverkehr zulässt, können Sie möglicherweise die Server in einem Subnetz finden, das ausgenommen ist, anstatt Ausnahmen für jede IP-Adresse zu verwenden.

Erstellen Sie wie beim Definieren der Grenz Zone einen formalen Prozess, um Hosts zu genehmigen, die der Ausnahmeliste hinzugefügt werden. Ein Modell für die Verarbeitung von Anforderungen für Ausnahmen finden Sie unter Entscheidungsfluss Diagramm im Abschnitt Grenz Zone .

Nächster Schritt: Isolierte Domäne

Isolierte Domäne

07.08.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die isolierte Domäne ist die primäre Zone für vertrauenswürdige Geräte. Die Geräte in dieser Zone verwenden Verbindungssicherheit und Firewallregeln, um die Kommunikation zu steuern, die zwischen Geräten in der Zone gesendet werden kann.

Der Begriff *Domäne* in diesem Kontext bezieht sich auf eine Grenze der Kommunikations Vertrauensstellung anstatt auf eine ActiveDirectory-Domäne. In dieser Lösung sind die beiden Konstrukte sehr ähnlich, da für die Annahme von eingehenden Verbindungen von vertrauenswürdigen Geräten die Active Directory-Domänenauthentifizierung (KerberosV5) erforderlich ist. Viele ActiveDirectory-Domänen (oder Gesamtstrukturen) können jedoch mit Vertrauensstellungen verknüpft werden, um eine einzelne, logische isolierte Domäne bereitzustellen. Darüber hinaus können Geräte, die sich mithilfe von Zertifikaten authentifizieren, auch in einer isolierten Domäne enthalten sein, ohne der Active Directory-Domäne beitreten zu müssen.

Bei den meisten Implementierungen enthält eine isolierte Domäne die größte Anzahl von Geräten. Andere Isolierungs Zonen können für die Lösung erstellt werden, wenn sich Ihre Kommunikationsanforderungen von denen der isolierten Domäne unterscheiden. Beispiele für diese Unterschiede sind die Ergebnisse der in diesem Leitfaden beschriebenen Grenz-und Verschlüsselungs Zonen. Konzeptionell handelt es sich bei der isolierten Domäne nur um die größte Isolierungs Zone und um eine Obermenge zu den anderen Zonen.

Sie müssen in Active Directory eine Gruppe erstellen, die Mitglieder der isolierten Domäne enthält. Anschließend wenden Sie eines von mehreren GPOs an, die Verbindungssicherheit und Firewallregeln für die Gruppe enthalten, damit die Authentifizierung für alle eingehenden Netzwerkverbindungen erzwungen wird. Die Erstellung der Gruppe und die Verknüpfung der GPOs, die die Regeln auf ihre Mitglieder anwenden, werden im Abschnitt Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen erläutert.

Die GPOs für die isolierte Domäne sollten die folgenden Verbindungssicherheitsregeln und-Einstellungen enthalten.

GPO-Einstellungen für isolierte Domänenmitglieder mit mindestens Windows Vista und Windows Server2008

GPOs für Geräte, die mindestens Windows Vista und Windows Server2008 ausführen, sollten Folgendes umfassen:

- IPsec-Standardeinstellungen, die die folgenden Optionen angeben:

  1. Befreien Sie den gesamten ICMP-Datenverkehr von IPSec.

  2. Schlüsselaustausch (Hauptmodus) Sicherheitsmethoden und-Algorithmus. Wir empfehlen, in Ihren Einstellungen mindestens DH4, AES und SHA2 zu verwenden. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.

  3. Algorithmus Kombinationen für den Datenschutz (Schnellmodus). Wir empfehlen, dass Sie des oder MD5 nicht in eine beliebige Einstellung einbeziehen. Sie sind nur zur Kompatibilität mit früheren Windows-Versionen enthalten. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle

unterstützten Betriebssysteme üblich sind.

Wenn NAT-Geräte in ihren Netzwerken vorhanden sind, verwenden Sie die ESP-Kapselung. Wenn isolierte Domänenmitglieder mit Hosts in der Verschlüsselungszone kommunizieren müssen, stellen Sie sicher, dass Sie Algorithmen einbeziehen, die mit den Anforderungen der Richtlinien für den Verschlüsselungsmodus kompatibel sind.

4. Authentifizierungsmethoden. Schließen Sie mindestens eine gerätebasierte KerberosV5-Authentifizierung ein. Wenn Sie benutzerbasierten Zugriff auf isolierte Server verwenden möchten, schließen Sie auch benutzerbasierte KerberosV5 als optionale Authentifizierungsmethode ein. Wenn eines ihrer isolierten Domänenmitglieder die KerberosV5-Authentifizierung nicht verwenden kann, schließen Sie die zertifikatbasierte Authentifizierung als optionale Authentifizierungsmethode ein.

- Die folgenden Verbindungssicherheitsregeln:
  - Eine Verbindungssicherheitsregel, mit der alle Geräte in der Ausnahmeliste von der Authentifizierung ausgenommen werden. Stellen Sie sicher, dass alle Active Directory-Domänencontroller in diese Liste aufgenommen werden. Geben Sie, sofern möglich, Subnet-Adressen anstelle diskreter Adressen ein, wenn dies in Ihrer Umgebung zutrifft.
  - Eine Verbindungssicherheitsregel von einer beliebigen IP-Adresse zu einer beliebigen, die eingehende und ausgehende Authentifizierung mithilfe der KerberosV5-Authentifizierung erfordert.

    > **Wichtig:** stellen Sie sicher, dass Sie die Vorgänge mithilfe von Anforderungs-und Anforderungs Verhalten beginnen, bis Sie sicher sind, dass alle Geräte in ihrer IPSec-Umgebung mithilfe von IPSec erfolgreich kommunizieren. Nachdem Sie bestätigt haben, dass IPSec wie erwartet funktioniert, können Sie die Richtlinie so ändern, dass Sie in erforderlich ist, anfordern.

- Eine Registrierungsrichtlinie, die die folgenden Werte enthält:
  - Aktivieren Sie die PMTU-Erkennung. Wenn Sie diese Einstellung aktivieren, kann TCP/IP die größte Paketgröße dynamisch ermitteln, die für eine Verbindung unterstützt wird. Der Wert wird unter HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\EnablePMTUDiscovery (DWORD) gefunden. Die XML-Beispieldatei für GPO-Einstellungen in Anhang A: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen legen den Wert auf **1**fest.

> **Hinweis:** eine Beispielvorlage für diese Registrierungseinstellungen finden Sie in Anhang a: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen.

Nächster Schritt: Grenzbereich

Begrenzungszone

01.06.2019 • 3 minutes to read

Betrifft

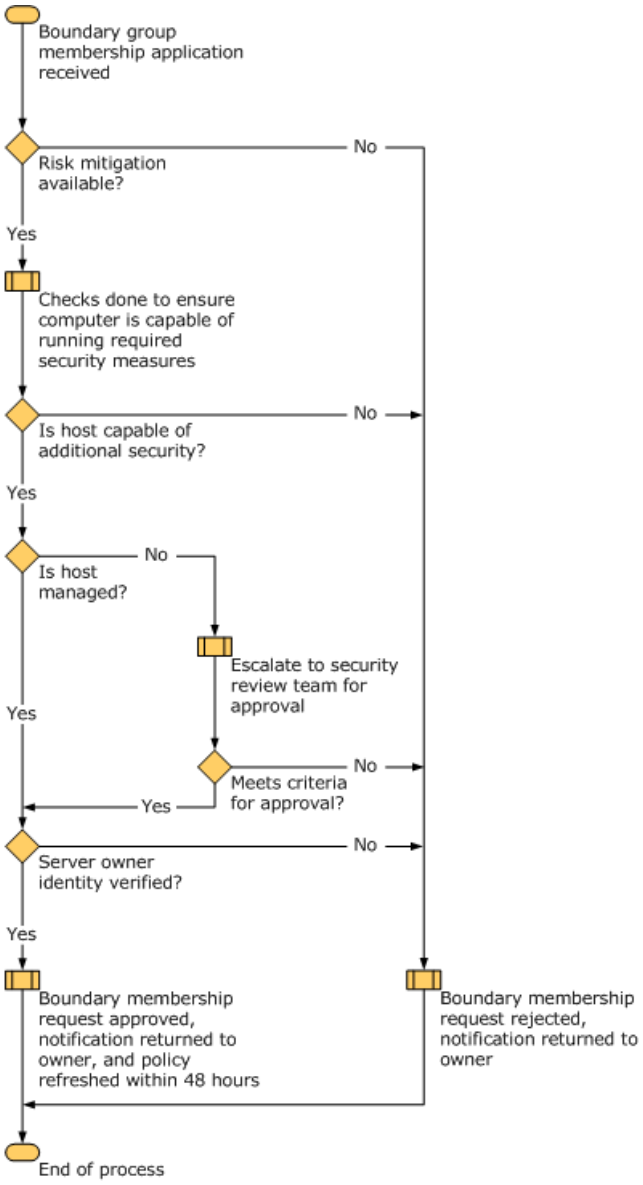
- Windows 10
- Windows Server 2016

In den meisten Organisationen müssen einige Geräte Netzwerkdatenverkehr von Geräten empfangen können, die nicht Teil der isolierten Domäne sind, und können daher nicht authentifiziert werden. Wenn Sie die Kommunikation von nicht vertrauenswürdigen Geräten akzeptieren möchten, erstellen Sie eine Grenz Zone innerhalb ihrer isolierten Domäne.

Geräte in der Grenz Zone sind vertrauenswürdige Geräte, die Kommunikationsanforderungen sowohl von anderen isolierten Domänenmitglieds Geräten als auch von nicht vertrauenswürdigen Geräten annehmen können. Grenzzonen Geräte versuchen Sie, eingehende Anforderungen mithilfe von IPSec zu authentifizieren, und initiieren Sie eine IKE-Aushandlung mit dem ursprünglichen Gerät.

Die für die Grenz Zone erstellten GPOs umfassen IPSec-oder Verbindungssicherheitsregeln, die eine Authentifizierung für eingehende und ausgehende Netzwerkverbindungen anfordern, diese aber nicht erfordern.

Da diese Grenzzonen Geräte unerwünschte eingehende Kommunikation von nicht vertrauenswürdigen Geräten empfangen können, die nur-Text verwenden, müssen Sie sorgfältig verwaltet und auf andere Weise gesichert werden. Das verringern dieses zusätzlichen Risikos ist ein wichtiger Bestandteil der Entscheidung, ob ein Gerät zur Grenz Zone hinzugefügt werden soll. Wenn Sie beispielsweise eine formelle geschäftliche Begründung durchführen, bevor Sie die einzelnen Geräte zur Grenz Zone hinzufügen, können Sie sicherstellen, dass das zusätzliche Risiko minimiert wird. Die folgende Abbildung zeigt ein Beispielverfahren, das eine solche Entscheidung erleichtern kann.



Das Ziel dieses Prozesses besteht darin, zu ermitteln, ob das Risiko des Hinzufügens eines Geräts zu einer Grenz Zone auf eine Ebene verringert werden kann, die es für die Organisation akzeptabel macht. Wenn das Risiko nicht gemildert werden kann, muss die Mitgliedschaft verweigert werden.

Sie müssen eine Gruppe in Active Directory erstellen, um die Mitglieder der Grenzzonen enthalten zu können. Die Einstellungen und Regeln für die Grenz Zone sind in der Regel sehr ähnlich wie bei der isolierten Domäne, und Sie können Zeit und Aufwand sparen, indem Sie diese GPOs kopieren, um Sie als Ausgangspunkt zu dienen. Der wichtigste Unterschied besteht darin, dass die Authentifizierungs Verbindungssicherheitsregel so festgesetzt werden muss, dass Sie die Authentifizierung für eingehenden und ausgehenden Datenverkehr anfordert, anstatt eine eingehende Authentifizierung zu erfordern und die ausgehende Authentifizierung wie von den isolierten Domäne.

Die Erstellung der Gruppe und die Verknüpfung mit den GPOs, die die Regeln auf Mitglieder der Gruppe anwenden, werden im Abschnitt Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen erläutert.

GPO-Einstellungen für Boundary Zone-Server mit mindestens Windows Server2008

Das Gruppenrichtlinienobjekt der Grenz Zone für Geräte, auf denen mindestens Windows Server2008 ausgeführt wird, sollte Folgendes umfassen:

- IPsec-Standardeinstellungen, die die folgenden Optionen angeben:

1. Befreien Sie den gesamten ICMP-Datenverkehr von IPSec.
2. Schlüsselaustausch (Hauptmodus) Sicherheitsmethoden und-Algorithmus. Wir empfehlen, in Ihren Einstellungen mindestens DH4, AES und SHA2 zu verwenden. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.
3. Algorithmus Kombinationen für den Datenschutz (Schnellmodus). Wir empfehlen, dass Sie des oder MD5 nicht in eine Einstellung aufnehmen. Sie sind nur zur Kompatibilität mit früheren Windows-Versionen enthalten. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.

   Wenn NAT-Geräte in ihren Netzwerken vorhanden sind, verwenden Sie die ESP-Kapselung. Wenn isolierte Domänenmitglieder mit Hosts in der Verschlüsselungszone kommunizieren müssen, stellen Sie sicher, dass Sie Algorithmen einbeziehen, die mit den Anforderungen der Richtlinien für den Verschlüsselungsmodus kompatibel sind.
4. Authentifizierungsmethoden. Schließen Sie mindestens eine gerätebasierte KerberosV5-Authentifizierung ein. Wenn Sie den benutzerbasierten Zugriff auf isolierte Server verwenden möchten, müssen Sie auch die benutzerbasierte KerberosV5-Authentifizierung als optionale Authentifizierungsmethode angeben. Wenn eine ihrer Domänen Isolierungs Mitglieder KerberosV5 nicht verwenden kann, müssen Sie auch die zertifikatbasierte Authentifizierung als optionale Authentifizierungsmethode angeben.

- Die folgenden Verbindungssicherheitsregeln:
  - Eine Verbindungssicherheitsregel, mit der alle Geräte in der Ausnahmeliste von der Authentifizierung ausgenommen werden. Stellen Sie sicher, dass alle Active Directory-Domänencontroller in diese Liste aufgenommen werden. Geben Sie die Subnet-Adressen ein, falls zutreffend in Ihrer Umgebung.
  - Eine Verbindungssicherheitsregel von **einer beliebigen IP-Adresse** zu **einer beliebigen IP-Adresse**, die eine eingehende und ausgehende Authentifizierung anfordert.
- Eine Registrierungsrichtlinie, die die folgenden Werte enthält:
  - Aktivieren Sie die PMTU-Erkennung. Wenn Sie diese Einstellung aktivieren, kann TCP/IP die größte Paketgröße dynamisch ermitteln, die für eine Verbindung unterstützt wird. Der Wert wird unter HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\EnablePMTUDiscovery (DWORD) gefunden. Die XML-Beispieldatei für GPO-Einstellungen in Anhang A: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen legen den Wert auf **1**fest.

> **Hinweis:** eine Beispielvorlage für diese Registrierungseinstellungen finden Sie in Anhang a: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen .

Nächster Schritt: Verschlüsselungs Zone

Verschlüsselungszone

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Einige Server in der Organisation hosten Daten, die sehr sensibel sind, einschließlich medizinischer, finanzieller oder anderer personenbezogener Daten. Behördliche oder Branchen rechtliche Vorschriften erfordern möglicherweise, dass diese vertraulichen Informationen verschlüsselt werden müssen, wenn Sie zwischen Geräten übertragen werden.

Um die zusätzlichen Sicherheitsanforderungen dieser Server zu unterstützen, empfehlen wir, dass Sie eine Verschlüsselungszone erstellen, die die Geräte enthält, und dass der vertrauliche eingehende und ausgehende Netzwerkdatenverkehr verschlüsselt werden muss.

Sie müssen in Active Directory eine Gruppe erstellen, die Mitglieder der Verschlüsselungszone enthalten soll. Die Einstellungen und Regeln für den Verschlüsselungsbereich sind in der Regel mit denen für die isolierte Domäne vergleichbar, und Sie können Zeit und Aufwand sparen, indem Sie diese GPOs kopieren, um Sie als Ausgangspunkt zu dienen. Anschließend ändern Sie die Liste der Sicherheitsmethoden so, dass nur Algorithmus Kombinationen mit Verschlüsselungsprotokollen enthalten sind.

Die Erstellung der Gruppe und die Verknüpfung mit den GPOs, die die Regeln auf Mitglieder der Gruppe anwenden, werden im Abschnitt Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen erläutert.

GPO-Einstellungen für Verschlüsselungs Zonenserver mit mindestens Windows Server2008

Das Gruppenrichtlinienobjekt für Geräte, auf denen mindestens Windows Server2008 ausgeführt wird, sollte Folgendes enthalten:

- IPsec-Standardeinstellungen, die die folgenden Optionen angeben:

  1. Befreien Sie den gesamten ICMP-Datenverkehr von IPSec.
  2. Schlüsselaustausch (Hauptmodus) Sicherheitsmethoden und-Algorithmus. Wir empfehlen, in Ihren Einstellungen mindestens DH4, AES und SHA2 zu verwenden. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.
  3. Algorithmus Kombinationen für den Datenschutz (Schnellmodus). Überprüfen Sie, ob **Verschlüsselung für alle Verbindungssicherheitsregeln erforderlich ist, die diese Einstellungen verwenden**, und geben Sie dann eine oder mehrere Kombinationen für Integrität und Verschlüsselung an. Wir empfehlen, dass Sie des oder MD5 nicht in eine Einstellung aufnehmen. Sie sind nur zur Kompatibilität mit früheren Windows-Versionen enthalten. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.

     Wenn NAT-Geräte in ihren Netzwerken vorhanden sind, verwenden Sie die ESP-Kapselung.
  4. Authentifizierungsmethoden. Schließen Sie mindestens eine gerätebasierte KerberosV5-Authentifizierung ein. Wenn Sie den benutzerbasierten Zugriff auf isolierte Server verwenden möchten, müssen Sie auch die benutzerbasierte KerberosV5-Authentifizierung als optionale Authentifizierungsmethode angeben. Wenn eine ihrer Domänen Isolierungs Mitglieder die

KerberosV5-Authentifizierung nicht verwenden kann, müssen Sie auch die zertifikatbasierte Authentifizierung als optionale Authentifizierungsmethode angeben.

- Die folgenden Verbindungssicherheitsregeln:
  - Eine Verbindungssicherheitsregel, mit der alle Geräte in der Ausnahmeliste von der Authentifizierung ausgenommen werden. Stellen Sie sicher, dass alle Active Directory-Domänencontroller in diese Liste aufgenommen werden. Geben Sie die Subnet-Adressen ein, falls zutreffend in Ihrer Umgebung.
  - Eine Verbindungssicherheitsregel von einer beliebigen IP-Adresse zu einer beliebigen, die eingehende und ausgehende Authentifizierung unter Verwendung der zuvor in dieser Richtlinie angegebenen Standardauthentifizierung erfordert.

    Wichtig stellen Sie sicher, dass Sie die Vorgänge mithilfe von Anforderungs-und Anforderungs Verhalten beginnen, bis Sie sicher sind, dass alle Geräte in ihrer IPSec-Umgebung mithilfe von IPSec erfolgreich kommunizieren. Nachdem Sie bestätigt haben, dass IPSec wie erwartet funktioniert, können Sie das Gruppenrichtlinienobjekt so ändern, dass es in erforderlich ist, anfordern.

- Eine Registrierungsrichtlinie, die die folgenden Werte enthält:
  - Aktivieren Sie die PMTU-Erkennung. Wenn Sie diese Einstellung aktivieren, kann TCP/IP die größte Paketgröße dynamisch ermitteln, die für eine Verbindung unterstützt wird. Der Wert wird unter HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\EnablePMTUDiscovery (DWORD) gefunden. Die XML-Beispieldatei für GPO-Einstellungen in Anhang A: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen legen den Wert auf **1**fest.

> **Hinweis:** eine Beispielvorlage für diese Registrierungseinstellungen finden Sie in Anhang a: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen.

- Wenn Domänenmitglieds Geräte mit Geräten in der Verschlüsselungszone kommunizieren müssen, stellen Sie sicher, dass Sie die Schnellmodus-Kombinationen von GPOs, die mit den Anforderungen der Verschlüsselungs Zonen-GPOs kompatibel sind, in die isolierten Domänengruppen einbeziehen.

Nächster Schritt: Planning Server-Isolierungs Zonen

Planen von Serverisolationszonen

07.08.2019 • 5 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Manchmal hostet ein Server vertrauliche Daten. Wenn Ihre Server Daten hosten, die nicht beeinträchtigt werden dürfen, stehen Ihnen mehrere Optionen zum Schutz dieser Daten zur Verfügung. Eine wurde bereits behandelt: Hinzufügen des Servers zur Verschlüsselungszone. Die Mitgliedschaft in dieser Zone verhindert, dass auf den Server von Geräten zugegriffen wird, die sich außerhalb der isolierten Domäne befinden, und verschlüsselt alle Netzwerkverbindungen mit dem Server.

Die zweite Möglichkeit besteht darin, den Zugriff auf den Server zusätzlich zu beschränken, nicht nur an Mitglieder der isolierten Domäne, sondern nur an die Benutzer oder Geräte, die geschäftliche Gründe haben, auf die Ressourcen auf dem Server zuzugreifen. Sie können nur genehmigte Benutzer angeben, oder Sie können zusätzlich angeben, dass die genehmigten Benutzer nur von zugelassenen Geräten aus auf den Server zugreifen können.

Um Access zu gewähren, fügen Sie die genehmigten Benutzer-und Geräte Konten zu Netzwerkzugriffsgruppen hinzu, auf die in einer Firewallregel auf diesem Server verwiesen wird. Wenn der Benutzer eine Anforderung an den Server sendet, werden die standardmäßigen Domänenisolationsregeln aufgerufen. Dies bewirkt, dass IKE KerberosV5 zum Austauschen von Anmeldeinformationen mit dem Server verwendet. Die zusätzliche Firewall-Regel auf dem Server veranlasst Windows, das bereitgestellte Gerät und die Benutzerkonten für die Gruppenmitgliedschaft in der Statusleiste zu überprüfen. Wenn der Benutzer oder das Gerät nicht Mitglied eines erforderlichen nag ist, wird die Netzwerkverbindung abgelehnt.

Isolierte Domänen und isolierte Server

Wenn Sie eine isolierte Domäne verwenden, verfügen die Clientgeräte bereits über die IPSec-Regeln, mit denen Sie den Datenverkehr authentifizieren können, wenn der Server dies erfordert. Wenn Sie einen isolierten Server hinzufügen, muss ein GPO auf seine Gruppe mit den entsprechenden Verbindungs Sicherheits-und Firewallregeln angewendet werden. Die Regeln erzwingen Authentifizierung und beschränken den Zugriff auf Verbindungen, die von einem autorisierten Gerät oder Benutzer authentifiziert werden.

Wenn Sie keine isolierte Domäne verwenden, aber dennoch einen Server isolieren möchten, der IPSec verwendet, müssen Sie die Clientgeräte konfigurieren, auf die Sie auf den Server zugreifen möchten, um die entsprechenden IPSec-Regeln zu verwenden. Wenn es sich bei den Clientgeräten um Mitglieder einer Active Directory-Domäne handelt, können Sie die Clients weiterhin mithilfe von Gruppenrichtlinien konfigurieren. Anstatt das Gruppenrichtlinienobjekt auf die gesamte Domäne anzuwenden, wenden Sie das Gruppenrichtlinienobjekt nur auf Mitglieder des nag an.

Erstellen mehrerer isolierter Server Zonen

Jede Gruppe von Servern, auf die von verschiedenen Gruppen von Benutzern zugegriffen werden muss, sollte in ihrer eigenen isolierten Serverzone eingerichtet werden. Nachdem eine Gruppe von GPOs für eine isolierte Serverzone erfolgreich erstellt und überprüft wurde, können Sie die GPOs in einen neuen Satz kopieren. Sie müssen die Namen der Gruppenrichtlinienobjekte so ändern, dass Sie die neue Zone, den Namen und die Mitgliedschaft der Gruppe der isolierten Serverzone, auf die die GPOs angewendet werden, und die Namen und die Mitgliedschaft der NAG-Gruppen, die bestimmen, welche Clients auf die Server in der isolierten Serverzone

zugreifen können, wiedergeben.

Erstellen der GPOs

Die Erstellung der Gruppen und deren Verknüpfung zu den GPOs, die die Regeln auf Mitglieder der Gruppen anwenden, werden im Abschnitt Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen erläutert.

Ein isolierter Server ist häufig ein Mitglied der Verschlüsselungszone. Daher dient das Kopieren dieser GPO-Gruppe als guter Ausgangspunkt. Anschließend ändern Sie die Regeln, um den Zugriff zusätzlich auf nag-Mitglieder zu beschränken.

GPO-Einstellungen für isolierte Server, auf denen mindestens Windows Server2008 ausgeführt wird

GPOs für Geräte mit mindestens Windows Server2008 sollten Folgendes umfassen:

> **Hinweis:** die hier beschriebenen Verbindungssicherheitsregeln sind mit denen für den Verschlüsselungsbereich identisch. Wenn Sie den Zugriff nicht verschlüsseln und auch den Zugriff auf nag-Member einschränken möchten, können Sie die Verbindungssicherheitsregeln verwenden, die mit der Haupt isolierten Domäne identisch sind. Sie müssen weiterhin die am Ende dieser Liste beschriebene Firewall-Regel hinzufügen, um Sie in eine isolierte Serverzone zu ändern.

- IPsec-Standardeinstellungen, die die folgenden Optionen angeben:

  1. Befreien Sie den gesamten ICMP-Datenverkehr von IPSec.
  2. Schlüsselaustausch (Hauptmodus) Sicherheitsmethoden und-Algorithmus. Wir empfehlen, dass Sie die Diffie-Hellman-Gruppe 1, des oder MD5 nicht in eine beliebige Einstellung einbeziehen. Sie sind nur zur Kompatibilität mit früheren Windows-Versionen enthalten. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.
  3. Algorithmus Kombinationen für den Datenschutz (Schnellmodus). Überprüfen Sie, ob **Verschlüsselung für alle Verbindungssicherheitsregeln erforderlich ist, die diese Einstellungen verwenden**, und geben Sie dann eine oder mehrere Kombinationen für Integrität und Verschlüsselung an. Wir empfehlen, dass Sie des oder MD5 nicht in eine Einstellung aufnehmen. Sie sind nur zur Kompatibilität mit früheren Windows-Versionen enthalten. Verwenden Sie die stärksten Algorithmus Kombinationen, die für alle unterstützten Betriebssysteme üblich sind.

     Wenn NAT-Geräte in ihren Netzwerken vorhanden sind, verwenden Sie AH nicht, weil NAT-Geräte nicht durchlaufen werden können. Wenn isolierte Server mit Hosts in der Verschlüsselungszone kommunizieren müssen, schließen Sie einen Algorithmus ein, der mit den Anforderungen der Verschlüsselungs Zonen-GPOs kompatibel ist.
  4. Authentifizierungsmethoden. Fügen Sie mindestens eine gerätebasierte KerberosV5-Authentifizierung zur Kompatibilität mit der restlichen isolierten Domäne hinzu. Wenn Sie den Zugriff auf bestimmte Benutzerkonten einschränken möchten, schließen Sie auch die benutzerbasierte KerberosV5-Authentifizierung als optionale Authentifizierungsmethode ein. Machen Sie die benutzerbasierte Authentifizierungsmethode nicht zwingend erforderlich, andernfalls können Geräte, die AuthIP anstelle von IKE nicht verwenden können, einschließlich WindowsXP und Windows Server2003, nicht kommunizieren. Wenn eine ihrer Domänen Isolierungs Mitglieder KerberosV5 nicht verwenden kann, schließen Sie die zertifikatbasierte Authentifizierung als optionale Authentifizierungsmethode ein.

- Die folgenden Regeln für die Verbindungssicherheit und Firewall:

  - Eine Verbindungssicherheitsregel, mit der alle Geräte in der Ausnahmeliste von der Authentifizierung ausgenommen werden. Stellen Sie sicher, dass alle Active Directory-Domänencontroller in diese Liste aufgenommen werden. Geben Sie die Subnet-Adressen ein, falls

zutreffend in Ihrer Umgebung.

- Eine Verbindungssicherheitsregel von **einer beliebigen IP-Adresse** zu **einer beliebigen IP-Adresse**, die eingehende und ausgehende Authentifizierung mithilfe der KerberosV5-Authentifizierung erfordert.

  > **Wichtig:** stellen Sie sicher, dass Sie die Vorgänge mithilfe von Anforderungs-und Anforderungs Verhalten beginnen, bis Sie sicher sind, dass alle Geräte in ihrer IPSec-Umgebung mithilfe von IPSec erfolgreich kommunizieren. Nachdem Sie bestätigt haben, dass IPSec wie erwartet funktioniert, können Sie das Gruppenrichtlinienobjekt so ändern, dass es in erforderlich ist, anfordern.

- Eine Firewallregel, die **nur sichere Verbindungen zulassen**angibt, **Verschlüsselung erfordert**, und auf der Registerkarte **Benutzer und Computer** enthält Verweise auf Geräte-und Benutzer Netzwerkzugriffsgruppen.

- Eine Registrierungsrichtlinie, die die folgenden Werte enthält:

  - Aktivieren Sie die PMTU-Erkennung. Wenn Sie diese Einstellung aktivieren, kann TCP/IP die größte Paketgröße dynamisch ermitteln, die für eine Verbindung unterstützt wird. Der Wert wird unter HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\EnablePMTUDiscovery (DWORD) gefunden. Die XML-Beispieldatei für GPO-Einstellungen in Anhang A: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen legen den Wert auf **1**fest.

> **Hinweis:** eine Beispielvorlage für diese Registrierungseinstellungen finden Sie in Anhang a: Beispieldateien für GPO-Vorlagen für die in diesem Leitfaden verwendeten Einstellungen.

Nächster Schritt: Planen der zertifikatbasierten Authentifizierung

Planen der zertifikatbasierten Authentifizierung

07.08.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Manchmal kann ein Gerät nicht an einer Active Directory-Domäne teilnehmen und kann daher keine KerberosV5-Authentifizierung mit Domänenanmeldeinformationen verwenden. Das Gerät kann jedoch mithilfe der zertifikatbasierten Authentifizierung weiterhin an der isolierten Domäne teilnehmen.

Der nicht-Domänenmitgliedsserver und die Clients, die mit dieser kommunizieren können müssen, müssen für die Verwendung von kryptografischen Zertifikaten auf der Grundlage des X. 509-Standards konfiguriert sein. Diese Zertifikate können als alternativer Satz von Anmeldeinformationen verwendet werden. Während der IKE-Aushandlung sendet jedes Gerät eine Kopie seines Zertifikats an das andere Gerät. Jedes Gerät überprüft das empfangene Zertifikat und überprüft dann seine Echtheit. Um als verbindlich zu gelten, muss das empfangene Zertifikat von einem Zertifizierungsstellenzertifikat im Speicher des vertrauenswürdigen Stammzertifizierungsstelle auf dem lokalen Gerät überprüft werden.

Zertifikate können von gewerblichen Unternehmen oder von einem internen Zertifikatserver erworben werden, der als Teil der Public Key-Infrastruktur (PKI) der Organisation eingerichtet wurde. Microsoft stellt eine vollständige PKI-und Zertifizierungsstellen Lösung mit Windows Server 2012, Windows Server2008R2 und Windows Server2008 Active Directory Certificate Services (MDE) bereit.

Bereitstellen von Zertifikaten

Unabhängig davon, wie Sie Ihre Zertifikate erwerben, müssen Sie diese auf Clients und Servern bereitstellen, die diese für die Kommunikation erforderlich machen.

Verwenden von Active Directory-Zertifikatdiensten

Wenn Sie MDE verwenden, um eigene Benutzer-und Gerätezertifikate intern zu erstellen, erstellen die als Zertifizierungsstellen benannten Server die Zertifikate basierend auf vom Administrator entworfenen Vorlagen. MDE verwendet dann Gruppenrichtlinien zum Bereitstellen der Zertifikate auf Domänenmitglieds Geräten. Gerätezertifikate werden bereitgestellt, wenn ein Domänenmitglieds Gerät gestartet wird. Benutzerzertifikate werden bereitgestellt, wenn sich ein Benutzer anmeldet.

Wenn Sie möchten, dass nicht-Domänenmitglieds Geräteteil einer Server Isolations Zone sind, für die nur autorisierte Benutzer Zugriff benötigen, stellen Sie sicher, dass Sie die Zertifikatzuordnung einbeziehen, um die Zertifikate bestimmten Benutzerkonten zuzuordnen. Wenn die Zertifikatzuordnung aktiviert ist, enthält das für jedes Gerät oder jeden Benutzer ausgestellte Zertifikat genügend Identifikationsinformationen, damit IPsec dem Zertifikat sowohl Benutzer-als auch Geräte Konten zugeordnet werden kann.

MDE stellt automatisch sicher, dass die von den CAS ausgestellten Zertifikate von den Clientgeräten als vertrauenswürdig eingestuft werden, indem die Zertifizierungsstellenzertifikate in den richtigen Speicher auf jedem Domänenmitglieds Gerät gesetzt werden.

Verwenden eines kommerziell gekauften Zertifikats für Geräte mit Windows

Sie können die Zertifikate manuell auf jedes Gerät importieren, wenn die Anzahl der Geräte relativ klein ist. Verwenden Sie für eine Bereitstellung für mehr als eine Handvoll von Geräten Gruppenrichtlinien.

Sie müssen zuerst das Stammzertifikat der Zertifizierungsstelle des Herstellers herunterladen und es dann in ein

GPO importieren, das es auf jedem Gerät, das das Gruppenrichtlinienobjekt anwendet, auf dem lokalen Computer\Trusted-Stammzertifizierungsstellen Speicher bereitstellt.

Sie müssen das gekaufte Zertifikat auch in ein GPO importieren, das es auf jedem Gerät, das das Gruppenrichtlinienobjekt anwendet, im lokalen Computer\Personal-Speicher bereitstellt.

Verwenden eines kommerziell gekauften Zertifikats für Geräte mit einem nicht-Windows-Betriebssystem

Wenn Sie die Zertifikate auf einem anderen Betriebssystem als Windows installieren, lesen Sie die Dokumentation zu diesem Betriebssystem.

Konfigurieren von IPSec für die Verwendung der Zertifikate

Wenn auf den Clients und Servern die Zertifikate zur Verfügung stehen, können Sie die IPSec-und Verbindungssicherheitsregeln so konfigurieren, dass diese Zertifikate als gültige Authentifizierungsmethode enthalten sind. Die Authentifizierungsmethode erfordert den Antragstellernamen des Zertifikats, beispielsweise: **DC = com, DC = woodgrovebank, CN = CorporateCertServer**. Wählen Sie optional **Zertifikat zur Kontozuordnung aktivieren** aus, um die Verwendung dieser Anmeldeinformationen zum Einschränken des Zugriffs auf Benutzer oder Geräte zu unterstützen, die Mitglieder von autorisierten Gruppen in einer Serverisolierungslösung sind.

Ab Windows Server 2012 können Sie Zertifikatauswahlkriterien so konfigurieren, dass das gewünschte Zertifikat ausgewählt und/oder validiert wird. Es können erweiterte Schlüssel Verwendungskriterien sowie Namenseinschränkungen und Zertifikat Fingerabdrücke konfiguriert werden. Diese Option wird über die Schaltfläche **erweitert** konfiguriert, wenn Sie Zertifikate für die Authentifizierungsmethode auf der Benutzeroberfläche oder über Windows PowerShell auswählen.

Nächster Schritt: Dokumentieren der Zonen

Dokumentieren der Zonen

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Im Allgemeinen ist die Aufgabe der Bestimmung der Zonen Mitgliedschaft nicht komplex, kann aber zeitaufwendig sein. Verwenden Sie die Informationen, die im Abschnitt Entwerfen einer Windows Defender-Firewall mit erweiterten Sicherheitsstrategien in diesem Leitfaden generiert wurden, um die Zone zu ermitteln, in der die einzelnen Hosts platziert werden. Sie können diese Zonen Platzierung dokumentieren, indem Sie eine Gruppenspalte zur Inventur Tabelle hinzufügen, die im Abschnitt Entwerfen einer Windows Defender-Firewall mit erweiterter Sicherheitsstrategie gezeigt wird. Hier sehen Sie ein Beispiel:

| Hostname | Hardware-reqs erfüllt | Software-reqs erfüllt | Konfiguration erforderlich | Details | Geplante Kosten | Gruppe | | - | - | - | - | - | - | | CLIENT001 | Nein| Nein| Aktualisieren von Hardware und Software.| Das aktuelle Betriebssystem ist WindowsXP. Alte Hardware ist mit neueren Versionen von Windows nicht kompatibel.| $??| Isolierte Domäne| | SERVER002 | Ja| Nein.| Teilnehmen an einer vertrauenswürdigen Domäne, Upgrade von Windows Server2008 auf mindestens Windows Server 2012| Keine Antivirus-Software vorhanden.| $??| Verschlüsselung| | SENSITIVE001 | Ja| Ja| Nicht erforderlich.| Ausführen von Windows Server 2012 Bereit für die Aufnahme.| $0| Isolierter Server (in Zone für sich selbst)| | PRINTSVR1 | Ja| Ja| Nicht erforderlich.| Ausführen von Windows Server2008R2 Bereit für die Aufnahme.| $0| Begrenzungslinie|

Nächster Schritt: Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen

Planen der Gruppenrichtlinienbereitstellung für die Netzwerkisolationszonen

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie sich für das beste logische Design Ihrer Isolierungs Umgebung für die Netzwerk-und Geräte Sicherheitsanforderungen entschieden haben, können Sie den Implementierungsplan starten.

Sie verfügen über eine Liste der Isolierungs Zonen mit den jeweiligen Sicherheitsanforderungen. Für die Implementierung müssen Sie die Gruppen planen, die die Geräte Konten in den einzelnen Zonen enthalten, die Netzwerkzugriffsgruppen, die verwendet werden, um zu ermitteln, wer auf einen isolierten Server zugreifen kann, und die GPOs mit den Verbindungs Sicherheits-und Firewallregeln, die für die Anwendung gelten sollen. entsprechenden Gruppen. Schließlich müssen Sie festlegen, wie Sie sicherstellen, dass die Richtlinien nur für die richtigen Geräte innerhalb der einzelnen Gruppen gelten.

- Planen von Isolationsgruppen für die Zonen
- Planen der Netzwerkzugriffsgruppen
- Planen der GPOs
- Planen der GPO-Bereitstellung

Planen von Isolationsgruppen für die Zonen

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Isolierungsgruppen in Active Directory sind, wie Sie die verschiedenen Domänen-und Server Isolations Zonen implementieren. Ein Gerät wird einer Zone zugewiesen, indem sein Geräte Konto der Gruppe hinzugefügt wird, die diese Zone repräsentiert.

> **Vorsicht:** fügen Sie Ihren Gruppen noch keine Geräte hinzu. Wenn sich ein Gerät in einer Gruppe befindet, wenn das Gruppenrichtlinienobjekt aktiviert ist, wird das Gruppenrichtlinienobjekt auf das Gerät angewendet. Wenn das Gruppenrichtlinienobjekt eine Authentifizierung erfordert und die anderen Geräte noch keine GPOs erhalten haben, kann das Gerät, das das neue Gruppenrichtlinienobjekt verwendet, möglicherweise nicht mit den anderen Personen kommunizieren.

Universelle Gruppen sind die beste Option für die Zuweisung von Gruppenrichtlinienobjekten, da Sie für die gesamte Gesamtstruktur gelten und die Anzahl der zu verwaltenden Gruppen reduzieren. Wenn jedoch universelle Gruppen nicht verfügbar sind, können Sie stattdessen globale Domänengruppen verwenden.

In der folgenden Tabelle sind die typischen Gruppen aufgeführt, die zum Verwalten der Domänen Isolations Zonen verwendet werden können, die im Beispiel der Woodgrove Bank in diesem Leitfaden erläutert werden:

GRUPPENNAME	BESCHREIBUNG
CG_DOMISO_No_IPsec	Eine universelle Gruppe von Geräte Konten, die nicht an der IPSec-Umgebung teilnehmen. Besteht in der Regel aus Infrastruktur-Device-Konten, die auch in Ausnahmelisten enthalten sind. Diese Gruppe wird in Sicherheitsgruppen Filtern verwendet, um sicherzustellen, dass GPOs mit IPSec-Regeln nicht auf Gruppenmitglieder angewendet werden.
CG_DOMISO_IsolatedDomain	Eine universelle Gruppe von Geräte Konten, die die Mitglieder der isolierten Domäne enthält. In den frühen Test Tagen kann diese Gruppe nur eine sehr geringe Anzahl von Geräten enthalten. Während der Produktion kann Sie die integrierte Gruppe " **Domänencomputer** " enthalten, um sicherzustellen, dass alle Geräte in der Domäne teilnehmen. Mitglieder dieser Gruppe erhalten das Gruppenrichtlinienobjekt für die Domänenisolierung, das für eingehende Verbindungen eine Authentifizierung erfordert.
CG_DOMISO_Boundary	Eine universelle Gruppe von Geräte Konten, die die Mitglieder der Grenz Zone enthält. Mitglieder dieser Gruppe erhalten ein GPO, das angibt, dass eine Authentifizierung angefordert, aber nicht erforderlich ist.

GRUPPENNAME	BESCHREIBUNG
CG_DOMISO_Encryption	Eine universelle Gruppe von Geräte Konten, die die Mitglieder der Verschlüsselungszone enthält. Mitglieder dieser Gruppe erhalten ein GPO, das angibt, dass für alle eingehenden Verbindungen sowohl Authentifizierung als auch Verschlüsselung erforderlich ist.
CG_SRVISO_*serverRole*	Eine universelle Gruppe von Geräte Konten, die die Mitglieder der Server Isolierungsgruppe enthält. Mitglieder dieser Gruppe erhalten das Server Isolations-GPO, das die Mitgliedschaft in einer Netzwerkzugriffsgruppe erfordert, um eine Verbindung herzustellen. Für jede Gruppe von Servern gibt es eine Gruppe mit unterschiedlichen Anforderungen für Benutzer-und Geräteeinschränkungen.

Mehrere GPOs werden möglicherweise an jede Gruppe übermittelt. Welche Anwendung tatsächlich angewendet wird, hängt von den Sicherheitsgruppen Filtern ab, die den GPOs zugewiesen sind, sowie den Ergebnissen der WMI-Filterung, die den GPOs zugewiesen ist. Details zum Layout des GPO werden im Abschnitt Planen der GPOserläutert.

Wenn einer Gruppe mehrere GPOs zugewiesen sind und ähnliche Regeln angewendet werden, ist die Regel, die dem Netzwerkverkehr am ehesten entspricht, diejenige, die vom Gerät verwendet wird. Wenn beispielsweise eine IPSec-Regel besagt, dass die Authentifizierung für den gesamten IP-Datenverkehr angefordert werden soll, und eine zweite Regel aus einem anderen Gruppenrichtlinienobjekt besagt, dass eine Authentifizierung für den IP-Datenverkehr zu und von einer bestimmten IP-Adresse erforderlich ist, hat die zweite Regel Vorrang, da Sie spezifischer ist.

Nächster Schritt: Planen von Netzwerkzugriffsgruppen

Planen der Netzwerkzugriffsgruppen

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Mithilfe einer Netzwerkzugriffsgruppe (NAG) werden Benutzer und Geräte identifiziert, die über die Berechtigung für den Zugriff auf einen isolierten Server verfügen. Der Server ist mit Firewallregeln konfiguriert, die nur Netzwerkverbindungen zulassen, die von einem Gerät authentifiziert werden, und optional ein Benutzer, dessen Konten Mitglieder des nag sind. Ein Mitglied der isolierten Domäne kann beliebig viele Benutzernamen aufweisen.

Verringern Sie die Anzahl der Problemlösungen, um die Komplexität der Lösung zu begrenzen. Sie benötigen eine NAG für jede Server Isolierungsgruppe, um die Geräte oder Benutzer zu beschränken, denen Zugriff gewährt wird. Optional können Sie den NAG in zwei unterschiedliche Gruppen aufteilen: einen für autorisierte Geräte und einen für autorisierte Benutzer.

Die von Ihnen erstellten und aufgefüllten Computer werden aktiv, indem Sie auf der Registerkarte **Benutzer und Computer** der Firewallregeln in dem Gruppenrichtlinienobjekt, das den isolierten Servern zugewiesen ist, darauf verweisen. Das Gruppenrichtlinienobjekt muss auch Verbindungssicherheitsregeln enthalten, die eine Authentifizierung erfordern, damit die Anmeldeinformationen für die nag-Mitgliedschaft überprüft werden.

Für das Woodgrove Bank-Szenario sind Zugriff auf die Geräte, auf denen SQL Server ausgeführt wird, die die WGBank-Anwendung unterstützen, auf die WGBank-Front-End-Server und die genehmigten administrativen Benutzer beschränkt, die bei bestimmten autorisierten administrativen Geräten angemeldet sind. Sie können auch nur von den genehmigten Administrator Benutzern und dem Dienstkonto abgerufen werden, das für den WGBank-Front-End-Dienst verwendet wird.

NAG-NAME	BENUTZER, COMPUTER ODER GRUPPEN VON NAG-MITGLIEDERN	BESCHREIBUNG
CG_NAG_*serverRole*_Users	Svr1AdminA Svr1AdminB Group_AppUsers AppSvcAccount	Diese Gruppe richtet sich an alle Benutzer, die berechtigt sind, eingehende IPSec-Verbindungen mit den isolierten Servern in dieser Zone zu führen.
CG_NAG_*serverRole*_Computers	Desktop1 Desktop2 AdminDT1 AppAdminDT1	Diese Gruppe enthält alle Geräte, die für eingehende IPSec-Verbindungen mit den isolierten Servern in dieser Zone autorisiert sind.

> **Hinweis:** die Mitgliedschaft in einem nag steuert nicht die Ebene des IPSec-Datenverkehrs Schutzes. Die IKE-Aushandlung ist sich nur bewusst, ob das Gerät oder der Benutzer den KerberosV5-Authentifizierungsprozess erfolgreich durchlaufen hat oder nicht. Die Verbindungssicherheitsregeln im angewendeten GPO steuern die Sicherheitsmethoden, die zum Schützen des Datenverkehrs verwendet werden, und sind unabhängig von der Identität, die von KerberosV5 authentifiziert wird.

Nächster Schritt: Planen der GPOs

Planen der GPOs

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie die GPOs für Ihre unterschiedlichen Isolierungs Zonen planen, müssen Sie das Layout der erforderlichen Zonen und deren Zuordnungen an die Gruppen vervollständigen, die die Geräte mit den Zonen verknüpfen.

Allgemeine Überlegungen

Einige Aspekte, die bei der Planung der GPOs zu Bedenken sind:

- Lassen Sie ein Gerät nicht Mitglied von mehr als einer Isolierungs Zone werden. Ein Gerät in mehr als einer Zone erhält mehrere und möglicherweise widersprüchliche GPOs. Dies kann zu unerwarteten und schwer zu behebenden Verhaltensweisen führen.

  Die Beispiele in diesem Leitfaden zeigen GPOs, die verhindern sollen, dass die Anforderung mehreren Zonen zugeordnet ist.

- Stellen Sie sicher, dass die IPsec-Algorithmen, die Sie in Ihren GPOs angeben, für alle Windows-Versionen kompatibel sind. Das gleiche Prinzip gilt für Daten Integritäts-und Verschlüsselungsalgorithmen. Wir empfehlen, die fortgeschritteneren Algorithmen einzubeziehen, wenn Sie die Möglichkeit haben, mehrere in einer sortierten Liste auszuwählen. Die Geräte werden am Anfang ihrer Listen ausgehandelt, wobei eine auf beiden Geräten konfigurierte Option ausgewählt wird.

- Der Hauptunterschied zwischen GPOs für Domänen Isolierungen besteht darin, ob die Regeln eine Authentifizierung anfordern oder erfordern.

  > **Vorsicht:** es ist **wichtig** , dass Sie zunächst alle GPOs so einrichten, dass Sie die Authentifizierung anfordern, anstatt Sie zu fordern. Da die GPOs über einen Zeitraum an die Geräte übermittelt werden, unterbricht die Anwendung einer require-Richtlinie auf ein Gerät die Möglichkeit zur Kommunikation mit einem anderen Gerät, das noch keine Richtlinie erhalten hat. Wenn Sie den Anforderungsmodus am Anfang verwenden, können Geräte weiterhin mithilfe von Klartext-Verbindungen kommunizieren, wenn dies erforderlich ist. Nachdem Sie bestätigt haben, dass Ihre Geräte IPSec in der erwarteten Weise verwenden, können Sie eine Konvertierung der Regeln in den GPOs planen, um eine Authentifizierung zu fordern, die für die einzelnen Zonen erforderlich ist.

- Die Windows Defender-Firewall * in Windows Vista und Windows Server2008 unterstützt nur jeweils ein Netzwerkstandort Profil. Wenn Sie einen zweiten Netzwerkadapter hinzufügen, der mit einem anderen Netzwerk verbunden ist oder überhaupt nicht verbunden ist, können Sie das aktuell auf dem Gerät aktive Profil versehentlich ändern. Wenn Ihr Gruppenrichtlinienobjekt unterschiedliche Firewall-und Verbindungssicherheitsregeln basierend auf dem aktuellen Netzwerkstandort Profil angibt, ändert sich das Verhalten, wie das Gerät den Netzwerkdatenverkehr verarbeitet, entsprechend. Für stationäre Geräte wie Desktops und Server empfehlen wir, allen Profilen eine beliebige Regel für das Gerät zuzuweisen. Wenden Sie GPOs an, die die Regeln pro Netzwerkstandort auf Geräte ändern, die zwischen Netzwerken, wie beispielsweise tragbaren Geräten, verschoben werden müssen. Erstellen Sie ein separates GPO für die Domänenisolierung für Ihre Server, das die gleichen Einstellungen wie das Gruppenrichtlinienobjekt für die

Clients verwendet, mit der Ausnahme, dass das Server-Gruppenrichtlinienobjekt dieselben Regeln für alle Netzwerkstandort Profile festlegt.

- Windows Defender Firewall heißt jetzt Windows Defender Firewall mit erweiterter Sicherheit in Windows 10.

> **NOTE**
> Geräte, auf denen Windows7, Windows Server2008R2 und höher ausgeführt wird, unterstützen unterschiedliche Netzwerkstandorttypen und daher Profile für jeden Netzwerkadapter gleichzeitig. Jedem Netzwerkadapter wird der Netzwerkstandort zugewiesen, der für das Netzwerk geeignet ist, mit dem er verbunden ist. Die Windows Defender-Firewall erzwingt dann nur die Regeln, die für das Profil dieses Netzwerktyps gelten. Daher werden bestimmte Arten von Datenverkehr blockiert, wenn Sie von einem Netzwerkadapter aus verbunden sind, der mit einem öffentlichen Netzwerk verbunden ist, aber diese Typen sind möglicherweise bei einem privaten oder Domänennetzwerk zulässig.

Nachdem Sie diese Probleme berücksichtigt haben, dokumentieren Sie jedes von Ihnen benötigte Gruppenrichtlinienobjekt und die Details zu den erforderlichen Verbindungssicherheit-und Firewall-Regeln.

Beispiel-GPOs für Woodgrove Bank

Im Beispiel der Woodgrove Bank wird die folgende Gruppe von GPOs verwendet, um die Domänen Isolierungsanforderungen zu unterstützen. In diesem Abschnitt werden nur die Regeln und Einstellungen für die Server-und Domänenisolierung erläutert. GPO-Einstellungen, die sich darauf auswirken, welche Geräte das Gruppenrichtlinienobjekt empfangen, wie beispielsweise die Filterung von Sicherheitsgruppen und die WMI-Filterung, werden im Abschnitt Planen von Gruppenrichtlinienobjekten erläutert.

In diesem Abschnitt finden Sie Informationen zu den folgenden Themen:

- Firewall-GPOs
- GPOs für isolierte Domäne
- GPOs für Begrenzungszone
- GPOs für Verschlüsselungszone
- GPOs für Serverisolation

Firewall-GPOs

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Alle Geräte im Netzwerk der Woodgrove Bank, die Windows ausführen, sind Teil der isolierten Domäne, mit Ausnahme von Domänencontrollern. Um Firewallregeln zu konfigurieren, wird das in diesem Abschnitt beschriebene Gruppenrichtlinienobjekt mit dem Domänencontainer in der Active Directory-OU-Hierarchie verknüpft und dann mithilfe von Sicherheitsgruppen Filtern und WMI-Filtern gefiltert.

Das für das Woodgrove Bank-Beispielszenario erstellte Gruppenrichtlinienobjekt umfasst Folgendes:

- GPO_DOMISO_Firewall

GPO_DOMISO_Firewall

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Dieses Gruppenrichtlinienobjekt wird mithilfe der Windows Defender-Firewall mit erweiterter Sicherheitsschnittstelle in den Bearbeitungstools für Gruppenrichtlinien verfasst. Der Abschnitt Benutzerkonfiguration des Gruppenrichtlinienobjekts ist deaktiviert. Sie soll nur für Geräte gelten, die mindestens Windows7 oder Windows Server2008.

Firewall-Einstellungen

Dieses GPO bietet die folgenden Einstellungen:

- Sofern nicht anders angegeben, gelten die hier beschriebenen Firewall-Regeln und-Einstellungen für alle Profile.
- Die Firewall ist aktiviert, wenn eingehende, nicht angeforderte Verbindungen blockiert und ausgehende Verbindungen zugelassen sind.
- Unter dem Domänenprofil werden in den Einstellungen **Benachrichtigungen an den Benutzer angezeigt**, **Lokale Firewallregeln angewendet**und **lokale Verbindungssicherheitsregeln gelten** auf **Nein**festgesetzt. Diese Einstellungen werden nur auf das Domänenprofil angewendet, da die Geräte nur dann eine Ausnahmeregel für ein erforderliches Programm von einem Gruppenrichtlinienobjekt empfangen können, wenn Sie mit der Domäne verbunden sind. Unter den Profilen Public und private sind diese Einstellungen auf **Ja**eingestellt.

  > **Hinweis:** durch Erzwingen dieser Einstellungen müssen Sie Firewall-Ausnahmen für Programme definieren, da der Benutzer ein neues Programm nicht manuell zulassen kann. Sie müssen die Ausnahmeregeln bereitstellen, indem Sie Sie diesem Gruppenrichtlinienobjekt hinzufügen. Wir empfehlen, diese Einstellungen erst zu aktivieren, nachdem Sie alle Ihre Anwendungen getestet und die resultierenden Regeln in einem Testlabor und dann auf Pilot Geräten getestet haben.

Firewall-Regeln

Dieses GPO bietet die folgenden Regeln:

- Integrierte Firewall-Regelgruppen sind so konfiguriert, dass die normalerweise erforderliche Netzwerkoperation unterstützt wird. Die folgenden Regelgruppen sind so eingestellt, **dass Sie die Verbindung zulassen**:
  - Kernnetzwerke
  - Datei-und Druckerfreigabe
  - Netzwerkermittlung
  - Remote Verwaltung
  - Remotedesktop

- Verwaltung von Remote Ereignisprotokollen
- Verwaltung von geplanten Remote Aufgaben
- Remote Dienstverwaltung
- Remote-Volume-Verwaltung
- Windows Defender Firewall-Remote Verwaltung
- Windows-Verwaltungsinstrumentation (WMI)
- Windows-Remoteverwaltung

- Eine Firewall-Ausnahmeregel, um erforderlichen Netzwerkdatenverkehr für das WGBank-dashboardprogramm zu ermöglichen. Diese eingehende Regel ermöglicht den Netzwerkdatenverkehr für das Programm "Dashboard. exe" im Ordner "%ProgramFiles%\WGBank". Die Regel wird auch so gefiltert, dass nur Datenverkehr auf Port 1551 zugelassen wird. Diese Regel wird nur auf das Domänenprofil angewendet.

Nächster Schritt: GPOs für isolierte Domänen

GPOs für isolierte Domäne

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Alle Geräte in der isolierten Domäne werden zur Gruppe CG_DOMISO_IsolatedDomain. hinzugefügt. Sie müssen mehrere GPOs erstellen, um sich mit dieser Gruppe auszurichten, eine für jedes Windows-Betriebssystem, das unterschiedliche Regeln oder Einstellungen aufweisen muss, um die grundlegende Funktion für isolierte Domänen zu implementieren, die sich in ihrer isolierten Domäne befindet. Dieser Gruppe werden für alle in diesem Abschnitt beschriebenen GPOs Lese-und Gruppenrichtlinienberechtigungen gewährt.

Jedes GPO verfügt über einen Sicherheitsgruppenfilter, der verhindert, dass das Gruppenrichtlinienobjekt auf Mitglieder der Gruppe GP_DOMISO_No_IPsec. Jedes GPO ist mit einem WMI-Filter verbunden, um sicherzustellen, dass das Gruppenrichtlinienobjekt nur auf die angegebene Version von Windows angewendet wird. Weitere Informationen finden Sie im Abschnitt Planen der GPO-Bereitstellung .

Zu den für die isolierte Domäne der Woodgrove Bank erstellten GPOs gehören die folgenden:

- GPO_DOMISO_IsolatedDomain_Clients
- GPO_DOMISO_IsolatedDomain_Servers

GPO_DOMISO_IsolatedDomain_Clients

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Dieses Gruppenrichtlinienobjekt wird mithilfe der Windows Defender-Firewall mit erweiterter Sicherheitsschnittstelle in den Bearbeitungstools für Gruppenrichtlinien verfasst. Der Abschnitt Benutzerkonfiguration des Gruppenrichtlinienobjekts ist deaktiviert. Sie soll nur auf Clientgeräte angewendet werden, auf denen Windows 8, Windows7 oder Windows Vista ausgeführt wird.

Da Clientgeräte manchmal portabel sein können, werden die Einstellungen und Regeln für dieses GPO nur auf das Domänenprofil angewendet.

Allgemeine Einstellungen

Dieses GPO bietet die folgenden Einstellungen:

- In diesem GPO sind keine Firewalleinstellungen enthalten. Die Woodgrove Bank hat separate GPOs für Firewalleinstellungen erstellt (siehe Abschnitt Firewall-GPOs), um Sie für alle Clients in allen Isolierungs Zonen mit minimaler redundanzfrei zugeben.
- Das ICMP-Protokoll ist von den Authentifizierungsanforderungen ausgenommen, um eine einfachere Netzwerkproblembehandlung zu unterstützen.
- Diffie-Hellman-Gruppe 2 wird als Schlüsselaustauschalgorithmus angegeben. Hierbei handelt es sich um den stärksten verfügbaren Algorithmus, der von allen Betriebssystemen unterstützt wird, die bei der Woodgrove Bank verwendet werden. Nachdem die Woodgrove Bank das Upgrade auf Windows-Versionen abgeschlossen hat, die stärkere Algorithmen unterstützen, können Sie die schwächeren Schlüsselaustauschalgorithmen entfernen und nur die stärkeren verwenden.
- Die Registrierungseinstellungen, die in der folgenden Tabelle aufgeführt sind. Weitere Informationen finden Sie in der Beschreibung der Registrierungseinstellungen in der isolierten Domäne.

EINSTELLUNG	WERT
Aktivieren der PMTU-Ermittlung	1
IPsec-Ausnahmen	3

- Die Kombinationen der Hauptmodus-Sicherheitsmethode in der Reihenfolge, die in der folgenden Tabelle aufgeführt ist.

INTEGRITÄT	VERSCHLÜSSELUNG
Secure Hash Algorithm (SHA-1)	Erweiterter Verschlüsselungs Standard (AES-128)
SHA-1	3DES

- Die folgenden Kombinationen von Sicherheitsdaten Integritätsalgorithmen im Schnellmodus in der

Reihenfolge, die in der folgenden Tabelle aufgeführt ist.

PROTOKOLL	INTEGRITÄT	SCHLÜSSELLEBENSDAUER (MINUTEN/KB)
ESP	SHA-1	60/100000

- Die Kombinationen aus Sicherheitsdaten Integrität und Verschlüsselungsalgorithmus im Schnellmodus in der Reihenfolge, die in der folgenden Tabelle aufgeführt ist.

PROTOKOLL	INTEGRITÄT	VERSCHLÜSSELUNG	SCHLÜSSELLEBENSDAUER (MINUTEN/KB)
ESP	SHA-1	AES-128	60/100000
ESP	SHA-1	3DES	60/100000

> **Hinweis:** verwenden Sie nicht den MD5-und des-Algorithmus in Ihren GPOs. Sie sind nur zur Kompatibilität mit früheren Windows-Versionen enthalten.

Verbindungssicherheitsregeln

Dieses GPO bietet die folgenden Regeln:

- Eine Verbindungssicherheitsregel mit dem Namen " **isolierte Domänenregel** " mit den folgenden Einstellungen:
  - Von **einer beliebigen IP-Adresse** zu **einer beliebigen IP-Adresse**.
  - Voraussetzungen für **eingehende und Anforderung für ausgehende** Authentifizierung

    > **Wichtig:** auf dieser und allen anderen GPOs, die eine Authentifizierung erfordern, wählte die Woodgrove Bank zunächst nur Authentifizierung aus. Nachdem Sie bestätigt haben, dass die Geräte erfolgreich mithilfe von IPSec kommuniziert haben, haben Sie die GPOs so geändert, dass eine Authentifizierung erforderlich ist.

  - Wählen Sie für die **ersten Authentifizierungsmethoden Computer KerberosV5** als primäre Methode aus. Hinzufügen einer zertifikatbasierten Authentifizierung von **DC = com, DC = woodgrovebank, CN = CorporateCertServer** für Geräte, die Windows nicht ausführen können oder der Domäne nicht beitreten können, aber weiterhin an der isolierten Domäne teilnehmen müssen.
  - Wählen Sie für die **zweite Authentifizierung Benutzer KerberosV5**aus, und aktivieren Sie dann das Kontrollkästchen **zweite Authentifizierung ist optional** .
- Eine Verbindungssicherheitsregel zum Ausschließen von Geräten, die sich in der Ausnahmeliste befinden, von der Authentifizierungsanforderung:
  - Die IP-Adressen aller Geräte in der Ausnahmeliste müssen einzeln unter **Endpunkt 2**hinzugefügt werden.
  - Der Authentifizierungsmodus ist auf **nicht authentifizieren**eingestellt.

Nächster Schritt: GPO_DOMISO_IsolatedDomain_Servers

GPO_DOMISO_IsolatedDomain_Servers

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Dieses Gruppenrichtlinienobjekt wird mithilfe der Windows Defender-Firewall-Oberfläche in den Bearbeitungstools für Gruppenrichtlinien verfasst. Der Abschnitt Benutzerkonfiguration des Gruppenrichtlinienobjekts ist deaktiviert. Sie soll nur auf Server Geräte angewendet werden, auf denen mindestens Windows Server2008 ausgeführt wird.

Da so viele Einstellungen und Regeln für dieses GPO für mindestens Windows Vista im Gruppenrichtlinienobjekt üblich sind, können Sie Zeit sparen, indem Sie den Windows Defender-Firewall-Teil des Gruppenrichtlinienobjekts für mindestens Windows Vista exportieren und in das Gruppenrichtlinienobjekt für mindestens Windows Server20 importieren. 08. Ändern Sie nach dem Importieren nur die hier angegebenen Elemente:

- Dieses GPO wendet alle Einstellungen auf alle Profile an: Domäne, Privat und öffentlich. Da es nicht zu erwarten ist, dass ein Server mobil ist und Netzwerke wechselt, verhindert das Konfigurieren des Gruppenrichtlinienobjekts auf diese Weise einen Netzwerkfehler oder das Hinzufügen eines neuen Netzwerkadapters, um das Gerät unbeabsichtigt zu einem öffentlichen Profil mit einem anderen Satz von Regeln zu wechseln (im Fall eines Servers mit Windows Server2008).

  > **Wichtig:** Windows Vista und Windows Server2008 unterstützen jeweils nur ein Netzwerkstandort Profil. Das Profil des am wenigsten sicheren Netzwerktyps wird auf das Gerät angewendet. Wenn Sie einen Netzwerkadapter an ein Gerät anfügen, das physisch nicht mit einem Netzwerk verbunden ist, ist der Standorttyp des öffentlichen Netzwerks dem Netzwerkadapter zugeordnet und auf das Gerät angewendet.

Nächster Schritt: Grenzzonen-GPOs

GPOs für Begrenzungszone

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Alle Geräte in der Grenz Zone werden zur Gruppe CG_DOMISO_Boundary. hinzugefügt. Sie müssen mehrere GPOs erstellen, um mit dieser Gruppe auszurichten, eine für jedes Betriebssystem, das Sie in ihrer Grenz Zone haben. Dieser Gruppe werden für die in diesem Abschnitt beschriebenen GPOs Lese-und Apply-Berechtigungen in Gruppenrichtlinien gewährt.

> **Hinweis:** Wenn Sie GPOs für mindestens Windows Vista oder Windows Server2008 entwerfen, können Sie Ihre GPOs in geschachtelten Gruppen entwerfen. So können Sie beispielsweise die umgrenzungs Gruppe zu einem Mitglied der Gruppe der isolierten Domänen machen, sodass Sie die Firewall und die grundlegenden Einstellungen für die isolierte Domäne über diese geschachtelte Mitgliedschaft erhält, wobei nur die Änderungen durch das Gruppenrichtlinienobjekt für Grenzzonen bereitgestellt werden. Aus Gründen der Einfachheit werden in diesem Leitfaden die Techniken beschrieben, mit denen unabhängige, nicht mehrschichtige Richtlinien erstellt werden. Wir empfehlen, dass Sie ein Skript erstellen und in regelmäßigen Abständen ausführen, das die Mitgliedschaften der Gruppen vergleicht, die sich gegenseitig ausschließen müssen, und Berichte über alle Geräte, die fälschlicherweise mehr als einer Gruppe zugeordnet sind.

Das bedeutet, dass Sie ein GPO für eine Grenzgruppe für ein bestimmtes Betriebssystem erstellen, indem Sie das entsprechende Gruppenrichtlinienobjekt für die isolierte Domäne kopieren und einfügen und dann die neue Kopie so ändern, dass das in der Grenz Zone erforderliche Verhalten bereitgestellt wird.

Die in diesem Leitfaden erörterten Grenzzonen-GPOs sind nur für Server Versionen von Windows vorgesehen, da nicht erwartet wird, dass Clientgeräte an der Grenz Zone teilnehmen. Wenn ein solches Erfordernis eintritt, erstellen Sie entweder ein neues Gruppenrichtlinienobjekt für diese Version von Windows, oder erweitern Sie den WMI-Filter, der an eines der vorhandenen Grenzzonen-GPOs angefügt ist, damit es auf die Client Version von Windows angewendet wird.

Im Beispiel der Woodgrove Bank werden nur die GPO-Einstellungen für einen Webdienst in mindestens Windows Server2008 erörtert.

- GPO_DOMISO_Boundary_WS2008

GPO_DOMISO_Boundary

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Dieses Gruppenrichtlinienobjekt wird mithilfe der Windows Defender-Firewall mit erweiterter Sicherheitsschnittstelle in den Bearbeitungstools für Gruppenrichtlinien verfasst. Die Woodgrove Bank hat mit dem Kopieren und Einfügen des Gruppenrichtlinienobjekts für die Windows Server2008-Version des Gruppenrichtlinienobjekts für isolierte Domänen begonnen und die Kopie dann umbenannt, um den neuen Zweck wiederzugeben.

Dieses GPO unterstützt die Möglichkeit für Geräte, die nicht Teil der isolierten Domäne sind, auf bestimmte Server zuzugreifen, die für diese nicht vertrauenswürdigen Geräte verfügbar sein müssen. Sie soll nur auf Server Geräte angewendet werden, auf denen mindestens Windows Server2008 ausgeführt wird.

IPSec-Einstellungen

Das kopierte GPO umfasst und verwendet weiterhin die IPSec-Einstellungen, mit denen Schlüsselaustausch-, Hauptmodus-und Schnellmodus-Algorithmen für die isolierte Domäne konfiguriert werden, wenn eine Authentifizierung verwendet werden kann.

Verbindungssicherheitsregeln

Benennen Sie die Regel der **isolierten Domäne** in **Grenzzonen Regel**um. Ändern Sie den Authentifizierungsmodus, um **eingehende und ausgehende Anfragen anzufordern**. In diesem Modus verwendet das Gerät eine Authentifizierung, wenn dies möglich ist, beispielsweise während der Kommunikation mit einem Mitglied der isolierten Domäne. Außerdem unterstützt Sie die "zurückgreifen auf klare" Fähigkeit des Anforderungsmodus, wenn ein nicht vertrauenswürdiges Gerät, das nicht Bestandteil der isolierten Domäne ist, eine Verbindung herstellt.

Registrierungseinstellungen

In der Grenz Zone werden die gleichen Registrierungseinstellungen wie für die isolierte Domäne verwendet, um den IPSec-Vorgang zu optimieren. Weitere Informationen finden Sie in der Beschreibung der Registrierungseinstellungen in der isolierten Domäne.

Firewall-Regeln

Kopieren Sie die Firewallregeln für die Grenz Zone aus dem Gruppenrichtlinienobjekt, das die Firewallregeln für die isolierte Domäne enthält. Passen Sie diese Kopie an, entfernen Sie Regeln für Dienste, die auf Servern in dieser Zone nicht benötigt werden, und fügen Sie eingehende Regeln hinzu, um den Netzwerkdatenverkehr für die Dienste zu ermöglichen, auf die von anderen Geräten aus zugegriffen werden soll. Die Woodgrove Bank hat beispielsweise eine Firewallregel hinzugefügt, um eingehenden Netzwerkdatenverkehr an den TCP-Port 80 für WebClient Anforderungen zu ermöglichen.

Stellen Sie sicher, dass das Gruppenrichtlinienobjekt, das Firewallregeln für die isolierte Domäne enthält, nicht auch auf die Grenz Zone angewendet wird, um überlappende und möglicherweise widersprüchliche Regeln zu verhindern.

Nächster Schritt: Verschlüsselungs Zonen-GPOs

GPOs für Verschlüsselungszone

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Behandeln Sie Verschlüsselungs Zonen auf ähnliche Weise wie die Grenzzonen. Ein Gerät wird einem Verschlüsselungsbereich hinzugefügt, indem das Geräte Konto zur Gruppe der Verschlüsselungs Zonen hinzugefügt wird. Die Woodgrove Bank verfügt über einen einzelnen Dienst, der geschützt werden muss, und die Geräte, die diesen Dienst ausführen, werden der Gruppe CG_DOMISO_Encryption. hinzugefügt. Dieser Gruppe wird in dem in diesem Abschnitt beschriebenen Gruppenrichtlinienobjekt die Berechtigung Lesen und Gruppenrichtlinien zuweisen gewährt.

Das Gruppenrichtlinienobjekt ist nur für Server Versionen von Windows vorgesehen. Es wird davon ausgegangen, dass Client Geräte am Verschlüsselungsbereich teilnehmen. Wenn ein solches Erfordernis eintritt, erstellen Sie entweder ein neues GPO für diese Version von Windows, oder erweitern Sie den WMI-Filter, der an eines der vorhandenen Verschlüsselungs Zonen-GPOs angefügt ist, damit es auf die Client Version von Windows angewendet wird.

- GPO_DOMISO_Encryption

GPO_DOMISO_Encryption_WS2008

07.08.2019 • 2 minutes to read

Dieses Gruppenrichtlinienobjekt wird mithilfe der Windows Defender-Firewall mit erweiterter Sicherheitsschnittstelle in den Bearbeitungstools für Gruppenrichtlinien verfasst. Die Woodgrove Bank hat mit dem Kopieren und Einfügen des Gruppenrichtlinienobjekts für die Windows Server2008-Version des Gruppenrichtlinienobjekts für isolierte Domänen begonnen und die Kopie dann umbenannt, um den neuen Zweck wiederzugeben.

Dieses GPO unterstützt die Möglichkeit, dass Server, die vertrauliche Daten enthalten, für alle Verbindungsanforderungen eine Verschlüsselung erfordern. Sie soll nur auf Server Computer angewendet werden, auf denen Windows Server 2012, Windows Server2008R2 oder Windows Server2008 ausgeführt wird.

IPSec-Einstellungen

Das kopierte GPO umfasst und verwendet weiterhin die IPSec-Einstellungen, die die Schlüsselaustausch-, Hauptmodus-und Schnellmodus-Algorithmen für die isolierte Domäne konfigurieren, wobei die folgenden Änderungen an der Verschlüsselungs Zonen Kopie des Gruppenrichtlinienobjekts vorgenommen werden:

Für die Verschlüsselungs Zonenserver müssen alle Verbindungen verschlüsselt werden. Ändern Sie dazu die IPsec-Standardeinstellungen für das Gruppenrichtlinienobjekt, damit die Einstellung **Verschlüsselung für alle Verbindungssicherheitsregeln erforderlich ist, die diese Einstellungen verwenden**. Dadurch werden alle Integritätsalgorithmus-Kombinationen deaktiviert.

Verbindungssicherheitsregeln

Benennen Sie die Regel für die **isolierte Domäne** in die **Verschlüsselungs Zonenregel**um. Belasse die Einstellung für den Authentifizierungsmodus auf **Inbound anfordern und ausgehende Anforderung**. In diesem Modus erzwingt der Computer die Authentifizierung für den gesamten eingehenden Netzwerkdatenverkehr und verwendet ihn, wenn er auf ausgehenden Datenverkehr zugreifen kann.

Registrierungseinstellungen

Die Verschlüsselungszone verwendet die gleichen Registrierungseinstellungen wie die isolierte Domäne zur Optimierung des IPSec-Vorgangs. Weitere Informationen finden Sie in der Beschreibung der Registrierungseinstellungen in der isolierten Domäne.

Firewall-Regeln

Kopieren Sie die Firewallregeln für den Verschlüsselungsbereich aus dem Gruppenrichtlinienobjekt, das die Firewallregeln für die isolierte Domäne enthält. Passen Sie diese Kopie an, entfernen Sie Regeln für Dienste, die auf Servern in dieser Zone nicht benötigt werden, und fügen Sie eingehende Regeln hinzu, um den Netzwerkdatenverkehr für die Dienste zu ermöglichen, auf die von anderen Computern zugegriffen werden soll. Die Woodgrove Bank hat beispielsweise eine Firewallregel hinzugefügt, um eingehenden Netzwerkdatenverkehr an TCP-Port 1433 für SQL Server-Clientanforderungen zu ermöglichen.

Ändern Sie die Aktion für jede eingehende Firewallregel, indem Sie zulassen, dass **die Verbindung nur sichere Verbindungen zulässt**, und wählen Sie dann **die zu verschlüsselten Verbindungen anfordern**aus.

Stellen Sie sicher, dass das Gruppenrichtlinienobjekt, das Firewallregeln für die isolierte Domäne enthält, nicht auch auf die Grenz Zone angewendet wird, um überlappende und möglicherweise widersprüchliche Regeln zu

verhindern.

Nächster Schritt: Server Isolierungs-GPOs

GPOs für Serverisolation

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Für jede Gruppe von Geräten, auf die unterschiedliche Benutzer oder Geräte zugreifen, ist eine separate Server Isolations Zone erforderlich. Für jede Zone ist für jede Windows-Version, die auf Geräten in der Zone ausgeführt wird, ein GPO erforderlich. Das Beispiel der Woodgrove Bank verfügt über eine Isolierungs Zone für Ihre Geräte, auf denen SQL Server ausgeführt wird. Die Server Isolations Zone wird logisch als Teil des Verschlüsselungs Bereichs angesehen. Daher müssen Server-Isolierungs Zonen-GPOs auch Regeln zum Verschlüsseln aller isolierten Server Datenverkehr umfassen. Die Woodgrove Bank hat die Verschlüsselungs Zonen-GPOs kopiert, um Sie als Ausgangspunkt zu verwenden, und hat sie umbenannt, damit Sie Ihren neuen Zweck widerspiegelt.

Alle Geräte Konten für Geräte in der SQL Server-Isolierungs Zone werden zur Gruppe CG_SRVISO_WGBANK_SQL. hinzugefügt. Dieser Gruppe werden für die in diesem Abschnitt beschriebenen GPOs Lese-und Gruppenrichtlinienberechtigungen gewährt. Die GPOs sind nur für Server Versionen von Windows verfügbar. Client Geräte werden nicht erwartet, dass Sie Mitglieder der Server Isolations Zone sind, obwohl Sie auf die Server in der Zone zugreifen können, indem Sie Mitglied einer Netzwerkzugriffsgruppe (NAG) für die Zone sind.

GPO_SRVISO

Dieses GPO ist mit dem GPO_DOMISO_Encryption-Gruppenrichtlinienobjekt mit den folgenden Änderungen identisch:

- Die Firewall-Regel, mit der die Verschlüsselung erzwungen wird, wird auf der Registerkarte **Benutzer und Computer** der Regel so geändert, dass Sie die "auf" enthält. Zu den für die Zugriffsrechte gewährten Berechtigungen gehören CG_NAG_SQL_Users und CG_NAG_SQL_Computers.

  > **Wichtig:** frühere Versionen von Windows unterstützen nur die gerätebasierte Authentifizierung. Wenn Sie angeben, dass die Benutzerauthentifizierung obligatorisch ist, können nur Benutzer auf Geräten, auf denen mindestens Windows Vista oder Windows Server2008 ausgeführt wird, eine Verbindung herstellen.

Nächster Schritt: Planen der GPO-Bereitstellung

Planen der GPO-Bereitstellung

01.06.2019 • 7 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Sie können in einer Kombination aus drei Methoden steuern, welche GPOs auf Geräte in Active Directory angewendet werden:

- **Active Directory-Organisationseinheitshierarchie** Dies umfasst das Verknüpfen des Gruppenrichtlinienobjekts mit einer bestimmten ou in der Active Directory-OU-Hierarchie. Alle Geräte in der OU und deren untergeordnete Container empfangen und übernehmen das Gruppenrichtlinienobjekt.

  Das Steuern der GPO-Anwendung durch Verknüpfen mit OUs wird in der Regel verwendet, wenn Sie die OU-Hierarchie entsprechend den Anforderungen Ihrer Domäne-Isolierungs Zone organisieren können. GPOs können Einstellungen auf Geräte basierend auf Ihrem Standort in Active Directory anwenden. Wenn ein Gerät von einer OU in eine andere verschoben wird, wird die mit der zweiten OU verknüpfte Richtlinie schließlich wirksam, wenn die Gruppenrichtlinie die Änderung während der Abfrage erkennt.

- **Filter für die Sicherheitsgruppe** Dies umfasst das Verknüpfen der GPOs mit der Domänenebene (oder einer anderen übergeordneten OU) in der OU-Hierarchie und das anschließende auswählen der Geräte, die das Gruppenrichtlinienobjekt empfangen, mithilfe von Berechtigungen, die nur richtigen Gruppenmitgliedern das Anwenden des Gruppenrichtlinienobjekts gestatten.

  Die Sicherheitsgruppenfilter sind an die GPOs selbst angefügt. Eine Gruppe wird dem Sicherheitsgruppenfilter des Gruppenrichtlinienobjekts in Active Directory hinzugefügt und dann Berechtigungen zum Lesen und Anwenden von Gruppenrichtlinien zugewiesen. Anderen Gruppen kann explizit die Berechtigung zum Lesen und Anwenden von Gruppenrichtlinien verweigert werden. Nur die Geräte, deren Gruppenmitgliedschaft die Berechtigung zum Lesen und Anwenden von Gruppenrichtlinien ohne explizite Verweigerungsberechtigungen erhält, können das Gruppenrichtlinienobjekt anwenden.

- **WMI-Filterung**. Ein WMI-Filter ist eine Abfrage, die dynamisch ausgeführt wird, wenn das Gruppenrichtlinienobjekt ausgewertet wird. Wenn ein Gerät ein Mitglied des Resultsets ist, wenn die WMI-Filterabfrage ausgeführt wird, wird das Gruppenrichtlinienobjekt auf das Gerät angewendet.

  Ein WMI-Filter besteht aus einer oder mehreren Bedingungen, die für das lokale Gerät ausgewertet werden. Sie können nahezu alle Merkmale des Geräts, das Betriebssystem und die installierten Programme überprüfen. Wenn alle angegebenen Bedingungen für das Gerät erfüllt sind, wird das Gruppenrichtlinienobjekt angewendet. Andernfalls wird das Gruppenrichtlinienobjekt ignoriert.

In diesem Leitfaden wird eine Kombination aus Sicherheitsgruppenfilterung und WMI-Filterung verwendet, um die flexibelsten Optionen bereitzustellen. Wenn Sie diese Anleitung befolgen, obwohl möglicherweise fünf unterschiedliche GPOs mit einer bestimmten Gruppe verbunden sind, weil Unterschiede bei der Betriebssystemversion auftreten, wird nur das richtige Gruppenrichtlinienobjekt angewendet.

Allgemeine Überlegungen

- Stellen Sie Ihre GPOs bereit, bevor Sie den Gruppen, die die GPOs empfangen, Geräte Konten hinzufügen. Auf diese Weise können Sie Ihre Geräte den Gruppen in kontrollierter Weise hinzufügen. Achten Sie darauf, zunächst nur ein paar Testgeräte hinzuzufügen. Überprüfen Sie vor dem Hinzufügen vieler Gruppenmitglieder

die Ergebnisse auf den Testgeräten, und überprüfen Sie, ob die konfigurierten Firewall-und Verbindungssicherheitsregeln den gewünschten Effekt aufweisen. In den folgenden Abschnitten finden Sie einige Vorschläge, was Sie testen sollten, bevor Sie fortfahren.

Testen der bereitgestellten Gruppen und GPOs

Nachdem Sie Ihre GPOs bereitgestellt und den Gruppen einige Testgeräte hinzugefügt haben, bestätigen Sie die folgenden Punkte, bevor Sie mit weiteren Gruppenmitgliedern fortfahren:

- Untersuchen Sie die Gruppenrichtlinienobjekte, die dem Gerät zugewiesen und von diesem gefiltert wurden. Führen Sie das **gpresult** -Tool an einer Eingabeaufforderung aus.
- Überprüfen Sie die auf dem Gerät bereitgestellten Regeln. Öffnen Sie das MMC-Snap-in Windows Defender-Firewall, erweitern Sie den Knoten **Überwachung** , und erweitern Sie dann die Knoten **Firewall** und **Verbindungssicherheit** .
- Überprüfen Sie, ob die Kommunikation authentifiziert ist. Öffnen Sie das MMC-Snap-in Windows Defender-Firewall, erweitern Sie den Knoten **Überwachung** , erweitern Sie den Knoten **Sicherheitszuordnungen** , und klicken Sie dann auf **Hauptmodus**.
- Überprüfen Sie, ob die Kommunikation verschlüsselt ist, wenn Sie von den Geräten benötigt wird. Öffnen Sie das MMC-Snap-in Windows Defender-Firewall, erweitern Sie den Knoten **Überwachung** , erweitern Sie den Knoten **Sicherheitszuordnungen** , und wählen Sie dann **Schnellmodus**aus. Für verschlüsselte Verbindungen wird in der Spalte **ESP-Vertraulichkeit** ein anderer Wert als **None** angezeigt.
- Stellen Sie sicher, dass Ihre Programme nicht betroffen sind. Führen Sie Sie aus, und bestätigen Sie, dass Sie weiterhin wie erwartet funktionieren.

Nachdem Sie bestätigt haben, dass die GPOs ordnungsgemäß angewendet wurden und die Geräte jetzt über den IPSec-Netzwerkdatenverkehr im Anforderungsmodus kommunizieren, können Sie mit dem Hinzufügen weiterer Geräte zu den Gruppenkonten in verwaltbaren Nummern beginnen. Fahren Sie mit dem überwachen und bestätigen der korrekten Anwendung der GPOs auf den Geräten fort.

Aktivieren Sie den require-Modus erst, wenn die Bereitstellung abgeschlossen ist.

Wenn Sie ein GPO bereitstellen, das eine Authentifizierung für ein Gerät erfordert, bevor die anderen Geräte ein GPO bereitgestellt haben, ist die Kommunikation zwischen diesen möglicherweise nicht möglich. Warten Sie, bis alle Zonen und Ihre GPOs im Anforderungsmodus bereitgestellt sind, und bestätigen Sie (wie im vorherigen Abschnitt beschrieben), dass die Geräte erfolgreich mithilfe von IPSec kommunizieren.

Wenn Probleme mit der Bereitstellung von Gruppenrichtlinienobjekten auftreten oder Fehler bei der Konfiguration eines oder mehrerer IPSec-GPOs auftreten, können Geräte weiterhin ausgeführt werden, da der Anforderungsmodus jedem Gerät das zurückgreifen auf eine klare Kommunikation ermöglicht.

Erst nachdem Sie alle Geräte zu ihren Zonen hinzugefügt haben und bestätigt haben, dass die Kommunikation wie erwartet funktioniert, können Sie mit dem Ändern der Regeln für den Anforderungsmodus beginnen, um Regeln für den Modus zu fordern, die in den Zonen erforderlich sind. Wir empfehlen, dass Sie den require-Modus in den Zonen eine Zone zu einem Zeitpunkt aktivieren, um zu bestätigen, dass Sie ordnungsgemäß funktionieren, bevor Sie fortfahren. Aktivieren Sie die Einstellung für den erforderlichen Modus für die Server Isolations Zonen zuerst, dann die Verschlüsselungszone und dann die isolierte Domäne.

Ändern Sie das GPO der Grenz Zone nicht, da es im Anforderungsmodus für eingehende und ausgehende Verbindungen bleiben muss.

Wenn Sie andere Zonen erstellen, für die ein eingehender oder ausgehender require-Modus erforderlich ist,

nehmen Sie die Einstellung so an, dass die Einstellung in Stufen von den kleineren Gruppen von Geräten auf die größeren Gruppen angewendet wird.

Beispiel für die Woodgrove Bank-Bereitstellungspläne

Die Woodgrove Bank verknüpft alle Ihre GPOs mit dem Container auf Domänenebene in der Active Directory-OU-Hierarchie. Anschließend werden die folgenden WMI-Filter und Sicherheitsgruppenfilter verwendet, um die Anwendung der GPOs auf die richtige Teilmenge von Geräten zu steuern. Für alle GPOs ist der Abschnitt Benutzerkonfiguration deaktiviert, um die Leistung zu verbessern.

GPO_DOMISO_Firewall

- **WMI-Filter**. Mit dem WMI-Filter kann dieses Gruppenrichtlinienobjekt nur auf Geräte angewendet werden, die mit der folgenden WMI-Abfrage übereinstimmen:

  ```
  select * from Win32_OperatingSystem where Version like "6.%" and ProductType <> "2"
  ```

  > **Hinweis:** Dies schließt Domänencontroller aus (die einen ProductType-Wert von 2 melden). Schließen Sie keine Domänencontroller in die isolierte Domäne ein, wenn Geräte mit einer älteren Version von Windows als Windows Vista und Windows Server2008 vorhanden sind.

- **Sicherheitsfilter**. Dieses GPO gewährt Lese-und Gruppenrichtlinienberechtigungen nur für Geräte, die Mitglieder der Gruppe CG_DOMISO_IsolatedDomain. sind. Das Gruppenrichtlinienobjekt verweigert auch explizit die Berechtigungen Lesen und Anwenden von Gruppenrichtlinien auf Mitglieder des CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Clients

- **WMI-Filter**. Mit dem WMI-Filter kann dieses Gruppenrichtlinienobjekt nur auf Geräte angewendet werden, die mit der folgenden WMI-Abfrage übereinstimmen:

  ```
  select * from Win32_OperatingSystem where Version like "6.%" and ProductType = "1"
  ```

- **Sicherheitsfilter**. Dieses GPO gewährt Lese-und Gruppenrichtlinienberechtigungen nur für Geräte, die Mitglieder der Gruppe CG_DOMISO_IsolatedDomain. sind. Das Gruppenrichtlinienobjekt verweigert auch explizit die Berechtigung zum Lesen und Anwenden von Gruppenrichtlinien für Mitglieder der Gruppe CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Servers

- **WMI-Filter**. Mit dem WMI-Filter kann dieses Gruppenrichtlinienobjekt nur auf Geräte angewendet werden, die mit der folgenden WMI-Abfrage übereinstimmen:

  ```
  select * from Win32_OperatingSystem where Version like "6.%" and ProductType = "3"
  ```

  > **Hinweis:** Dies schließt Domänencontroller aus (die einen ProductType-Wert von 2 melden). Schließen Sie keine Domänencontroller in die isolierte Domäne ein, wenn es Geräte gibt, auf denen Windows-Versionen vor Windows Vista und Windows Server2008 ausgeführt werden.

- **Sicherheitsfilter**. Dieses GPO gewährt Lese-und Gruppenrichtlinienberechtigungen nur für Geräte, die Mitglieder der Gruppe CG_DOMISO_IsolatedDomain. sind. Das Gruppenrichtlinienobjekt verweigert auch explizit die Berechtigung zum Lesen und Anwenden von Gruppenrichtlinien für Mitglieder der Gruppe CG_DOMISO_NO_IPSEC.

GPO_DOMISO_Boundary

- **WMI-Filter**. Mit dem WMI-Filter kann dieses Gruppenrichtlinienobjekt nur auf Geräte angewendet werden, die mit der folgenden WMI-Abfrage übereinstimmen:

```
select * from Win32_OperatingSystem where Version like "6.%" and ProductType = "3"
```

> **Hinweis:** Dies schließt Domänencontroller aus (die einen ProductType-Wert von 2 melden). Schließen Sie keine Domänencontroller in die isolierte Domäne ein, wenn es Geräte gibt, auf denen Windows-Versionen vor Windows Vista und Windows Server2008 ausgeführt werden.

- **Sicherheitsfilter**. Dieses GPO gewährt Lese-und Gruppenrichtlinienberechtigungen nur für Geräte, die Mitglieder der Gruppe CG_DOMISO_Boundary. sind. Das Gruppenrichtlinienobjekt verweigert auch explizit die Berechtigung zum Lesen und Anwenden von Gruppenrichtlinien für Mitglieder der Gruppe CG_DOMISO_NO_IPSEC.

GPO_DOMISO_Encryption

- **WMI-Filter**. Mit dem WMI-Filter kann dieses Gruppenrichtlinienobjekt nur auf Geräte angewendet werden, die mit der folgenden WMI-Abfrage übereinstimmen:

```
select * from Win32_OperatingSystem where Version like "6.%" and ProductType = "3"
```

> **Hinweis:** Dies schließt Domänencontroller aus (die einen ProductType-Wert von 2 melden). Schließen Sie keine Domänencontroller in die isolierte Domäne ein, wenn es Geräte gibt, auf denen Windows-Versionen vor Windows Vista und Windows Server2008 ausgeführt werden.

- **Sicherheitsfilter**. Dieses Gruppenrichtlinienobjekt gewährt Lese-und Apply-Berechtigungen nur für Geräte, die Mitglieder der Gruppe CG_DOMISO_Encryption. sind. Das Gruppenrichtlinienobjekt verweigert auch explizit Lese-und Apply-Berechtigungen in Gruppenrichtlinien für Mitglieder der Gruppe CG_DOMISO_NO_IPSEC.

AnhangA: GPO-Beispielvorlagendateien für die in diesem Handbuch verwendeten Einstellungen

07.08.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Sie können eine XML-Datei mit angepassten Registrierungseinstellungen in ein Gruppenrichtlinienobjekt (GPO) importieren, indem Sie das Feature Einstellungen der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) verwenden.

Um die Datei manuell zu erstellen, erstellen Sie die Einstellungen unter **Computer Konfiguration**, Einstellungen, **Windows-Einstellungen**, **Registrierung**. **** Nachdem Sie die Einstellungen erstellt haben, ziehen Sie den Container auf den Desktop. Dort wird eine XML-Datei erstellt.

Wenn Sie eine XML-Datei in die GPMC importieren möchten, ziehen Sie Sie, und legen Sie Sie auf dem **Registrierungs** Knoten unter **Computer Konfiguration**, **Einstellungen**, **Windows-Einstellungen**ab. Wenn Sie den folgenden XML-Beispielcode in eine Datei kopieren und dann auf dem **Registrierungs** Knoten ziehen und ablegen, wird eine **Server-und Domänen Isolierungs** Sammlung mit den sechs in diesem Leitfaden besprochenen Registrierungsschlüsseln erstellt.

In der folgenden Beispieldatei wird die Zielgruppenadressierung auf Elementebene verwendet, um sicherzustellen, dass die Registrierungsschlüssel nur auf die Windows-Versionen angewendet werden, auf die Sie zutreffen.

> **Hinweis:** die hier gezeigte Datei dient nur zur Stichproben Verwendung. Sie sollte so angepasst werden, dass Sie den Anforderungen der Bereitstellung Ihrer Organisation entspricht. Wenn Sie diese Datei anpassen möchten, importieren Sie Sie in ein Test-Gruppenrichtlinienobjekt, ändern Sie die Einstellungen, und ziehen Sie dann den Knoten Server-und Domänen Isolationseinstellungen auf Ihren Desktop. Die neue Datei enthält alle Ihre Anpassungen.

```
<?xml version="1.0" encoding="utf-8"?>

<Collection clsid="{53B533F5-224C-47e3-B01B-CA3B3F3FF4BF}" name="Server and Domain Isolation Settings">

<Registry
         clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}"
         name="Enable PMTU Discovery"
         status="EnablePMTUDiscovery"
         image="12"
         changed="2008-05-30 20:37:37"
         uid="{52C38FD7-A081-404C-A8EA-B24A9614D0B5}"
         desc="&lt;b&gt;Enable PMTU Discovery&lt;/b&gt;&lt;p&gt;
            This setting configures whether computers can use PMTU
            discovery on the network.&lt;p&gt;
            &lt;b&gt;1&lt;/b&gt; --  Enable&lt;br&gt;
            &lt;b&gt;0&lt;/b&gt; --  Disable"
         bypassErrors="1">
   <Properties
         action="U"
         displayDecimal="1"
         default="0"
         hive="HKEY_LOCAL_MACHINE"
         key="System\CurrentControlSet\Services\TCPIP\Parameters"
         name="EnablePMTUDiscovery" type="REG_DWORD" value="00000001"/>
</Registry>

<Registry
         clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}"
         name="IPsec Default Exemptions (Vista and W2K8)"
         status="NoDefaultExempt"
         image="12"
         changed="2008-05-30 20:33:32"
         uid="{AE5C505D-283E-4060-9A55-70659DFD56B6}"
         desc="&lt;b&gt;IPsec Default Exemptions for Windows Server 2008
            and later&lt;/b&gt;&lt;p&gt;
            This setting determines which network traffic type is exempt
            from any IPsec authentication requirements.&lt;p&gt;
            &lt;b&gt;0&lt;/b&gt;: Exempts multicast, broadcast, RSVP, Kerberos, ISAKMP&lt;br&gt;
            &lt;b&gt;1&lt;/b&gt;: Exempts multicast, broadcast, ISAKMP&lt;br&gt;
            &lt;b&gt;2&lt;/b&gt;: Exempts RSVP, Kerberos, ISAKMP&lt;br&gt;
            &lt;b&gt;3&lt;/b&gt;: Exempts ISAKMP only"
         bypassErrors="1">
   <Properties
         action="U"
         displayDecimal="1"
         default="0"
         hive="HKEY_LOCAL_MACHINE"
         key="SYSTEM\CurrentControlSet\Services\PolicyAgent"
         name="NoDefaultExempt"
         type="REG_DWORD"
         value="00000003"/>
   <Filters>
      <FilterOs
         bool="AND" not="0"
         class="NT" version="VISTA"
         type="NE" edition="NE" sp="NE"/>
      <FilterOs
         bool="OR" not="0"
         class="NT" version="2K8"
         type="NE" edition="NE" sp="NE"/>
   </Filters>
</Registry>

</Collection>
```

Windows Defender-Firewall mit erweitertem Sicherheits Bereitstellungshandbuch

04.12.2019 • 3 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Sie können das MMC-Snap-in Windows Defender-Firewall mit erweiterter Sicherheit mit Geräten verwenden, die mindestens Windows Vista oder Windows Server2008, um die Geräte und die Daten zu schützen, die Sie über ein Netzwerk freigeben.

Sie können die Windows Defender-Firewall verwenden, um den Zugriff auf das Gerät aus dem Netzwerk zu steuern. Sie können Regeln erstellen, die den Netzwerkverkehr in beiden Richtungen basierend auf Ihren geschäftlichen Anforderungen zulassen oder blockieren. Sie können auch IPsec-Verbindungssicherheitsregeln erstellen, um Ihre Daten zu schützen, während Sie über das Netzwerk von Gerät zu Gerät übertragen werden.

Informationen zu diesem Leitfaden

Dieser Leitfaden ist für die Verwendung durch Systemadministratoren und Systemingenieure vorgesehen. Sie enthält detaillierte Anleitungen für die Bereitstellung einer Windows Defender-Firewall mit erweitertem Sicherheitsdesign, die Sie oder ein Infrastrukturspezialist oder Systemarchitekt in Ihrer Organisation ausgewählt haben.

Überprüfen Sie zunächst die Informationen in Planen der Bereitstellung der Windows Defender-Firewall mit erweiterter Sicherheit.

Wenn Sie noch kein Design ausgewählt haben, empfehlen wir, dass Sie die Anweisungen in diesem Leitfaden erst befolgen, nachdem Sie die Entwurfsoptionen im Design Handbuch für Windows Defender-Firewall mit erweiterter Sicherheit überprüft und das für Ihre Organisation am besten geeignete ausgewählt haben.

Nachdem Sie Ihr Design ausgewählt und die erforderlichen Informationen zu den Zonen (Isolierung, Grenze und Verschlüsselung), zu unterstützende Betriebssysteme und weitere Details gesammelt haben, können Sie diese Anleitung verwenden, um Ihre Windows Defender-Firewall mit erweiterter Sicherheit bereitzustellen. Design in Ihrer Produktionsumgebung Dieses Handbuch enthält die Schritte zum Bereitstellen eines der folgenden primären Designs, die im Entwurfshandbuch beschrieben sind:

- Entwurf einer allgemeinen Firewallrichtlinie
- Entwurf einer Domänenisolationsrichtlinie
- Entwurf einer Serverisolationsrichtlinie
- Entwurf einer zertifikatbasierten Isolationsrichtlinie

Verwenden Sie die Checklisten in Implementieren Ihrer Windows Defender-Firewall mit dem erweiterten Sicherheitsentwurfs Plan , um zu ermitteln, wie Sie die Anweisungen in diesem Leitfaden für die Bereitstellung Ihres speziellen Designs optimal verwenden können.

> **Vorsicht:** es wird empfohlen, die in diesem Leitfaden dokumentierten Techniken nur für GPOs zu verwenden, die für die Mehrzahl der Geräte in Ihrer Organisation bereitgestellt werden müssen, und nur, wenn die OU-Hierarchie in Ihrer Active Directory-Domäne nicht den Bereitstellungsanforderungen dieser GPOs entspricht.

> Diese Merkmale sind typisch für GPOs für Server-und Domänen Isolierungs Szenarien, sind aber nicht für die meisten anderen GPOs typisch. Wenn die OU-Hierarchie Sie unterstützt, stellen Sie ein GPO bereit, indem Sie es mit der Organisationseinheit der niedrigsten Ebene verknüpfen, die alle Konten enthält, für die das Gruppenrichtlinienobjekt gilt.

In einer großen Unternehmensumgebung mit Hunderten oder Tausenden von GPOs kann die Verwendung dieses Verfahrens mit zu vielen GPOs zu Benutzer-oder Geräte Konten führen, die Mitglieder einer übermäßigen Anzahl von Gruppen sind. Dies kann zu Netzwerkverbindungsproblemen führen, wenn Netzwerkprotokoll Grenzwerte überschritten werden.

Was dieses Handbuch nicht bietet

Dieses Handbuch bietet keine:

- Leitfaden zum Erstellen von Firewallregeln für bestimmte Netzwerkanwendungen Diese Informationen finden Sie unter Planen von Einstellungen für eine grundlegende Firewall-Richtlinie im Entwurfshandbuch für Windows Defender-Firewall mit erweiterter Sicherheit.
- Leitfaden zum Einrichten von Active Directory-Domänendiensten (Adds) zur Unterstützung von Gruppenrichtlinien.
- Leitfaden zum Einrichten von Zertifizierungsstellen zum Erstellen von Zertifikaten für die zertifikatbasierte Authentifizierung.

Übersicht über die Windows Defender-Firewall mit erweiterter Sicherheit

Die Windows Defender-Firewall unter Windows 8, Windows7, Windows Vista, Windows Server 2012, Windows Server2008 und Windows Server2008R2 ist eine Stateful-Hostfirewall, die Ihnen hilft, das Gerät zu sichern, indem Sie Regeln erstellen, die den Netzwerkdatenverkehr ermitteln. zulässig, das Gerät aus dem Netzwerk einzugeben, und der Netzwerkdatenverkehr, das das Gerät an das Netzwerk senden darf. Die Windows Defender-Firewall unterstützt auch IPSec (Internet Protocol Security), die Sie verwenden können, um die Authentifizierung von jedem Gerät aus zu fordern, das mit Ihrem Gerät kommunizieren möchte. Wenn eine Authentifizierung erforderlich ist, können Geräte, die nicht als vertrauenswürdiges Gerät authentifiziert werden können, nicht mit Ihrem Gerät kommunizieren. Sie können IPSec auch dazu verwenden, bestimmte Netzwerkdaten zu verschlüsseln, um zu verhindern, dass Sie von Netzwerkpaket Analysatoren gelesen werden, die von einem böswilligen Benutzer an das Netzwerk angefügt werden können.

Das MMC-Snap-in Windows Defender Firewall mit erweiterter Sicherheit ist flexibler und bietet viel mehr Funktionalität als die verbraucherfreundliche Windows Defender-Firewall-Oberfläche, die in der Systemsteuerung zu finden ist. Beide Schnittstellen interagieren mit denselben zugrunde liegenden Diensten, bieten aber unterschiedliche Steuerungsebenen für diese Dienste. Zwar kann das Windows Defender Firewall Control Panel-Programm ein einzelnes Gerät in einer häuslichen Umgebung schützen, es bietet jedoch nicht genügend zentralisierte Verwaltungs-oder Sicherheitsfeatures, um einen komplexeren Netzwerkdatenverkehr in einem typischen Unternehmen zu gewährleisten. Umgebung.

Weitere Informationen zur Windows Defender-Firewall mit erweiterter Sicherheit finden Sie unter Windows Defender-Firewall mit erweiterter Sicherheit (Übersicht).

Planen der Bereitstellung der Windows Defender-Firewall mit erweiterter Sicherheit

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Nachdem Sie Informationen zu Ihrer Umgebung gesammelt und sich für ein Design entschieden haben, indem Sie die Anleitungen im Windows Defender Firewall mit Advanced Security Design Guidebefolgen, können Sie mit der Planung der Bereitstellung Ihres Entwurfs beginnen. Mit dem fertigen Design und den Informationen in diesem Thema können Sie ermitteln, welche Aufgaben ausgeführt werden müssen, um die Windows Defender-Firewall mit erweiterter Sicherheit in Ihrer Organisation bereitzustellen.

Überprüfen der Windows Defender-Firewall mit erweitertem Sicherheits Design

Wenn das Design Team, das das Windows Defender-Firewall-Design für Ihre Organisation erstellt hat, anders als das Bereitstellungsteam ist, das es implementieren soll, stellen Sie sicher, dass das Bereitstellungsteam das endgültige Design mit dem Entwurfsteam überprüft. Überprüfen Sie die folgenden Punkte:

- Die Strategie des Entwurfsteams, um zu ermitteln, wie WMI-und Sicherheitsgruppenfilter an die GPOs angefügt werden, bestimmt, welche Geräte für welches GPO gelten. Das Bereitstellungsteam kann auf die folgenden Themen im Design Handbuch für Windows Defender-Firewall mit erweiterter Sicherheit verweisen:
  - Planen von Isolationsgruppen für die Zonen
  - Planen der GPOs
  - Planen der GPO-Bereitstellung
- Die Kommunikation zwischen Mitgliedern der einzelnen Zonen in der isolierten Domäne und Geräten, die nicht Teil der isolierten Domäne oder Mitgliedern der Ausnahmeliste der isolierten Domäne sind, zulässig ist.
- Die Empfehlung, dass Domänencontroller von den IPSec-Authentifizierungsanforderungen ausgenommen werden. Wenn Sie nicht freigestellt sind und die Authentifizierung fehlschlägt, können Domänenclients möglicherweise keine Gruppenrichtlinienupdates für die IPsec-Verbindungssicherheitsregeln von den Domänencontrollern empfangen.
- Die Begründung für die Konfiguration aller IPSec-Authentifizierungsregeln zum Anfordern und nicht anfordern von Authentifizierung, bis die erfolgreiche Aushandlung von IPSec bestätigt wurde. Wenn die Regeln so festgesetzt sind, dass eine Authentifizierung erforderlich ist, bevor Sie bestätigen, dass die Authentifizierung ordnungsgemäß funktioniert, schlägt die Kommunikation zwischen Geräten möglicherweise fehl. Wenn die Regeln nur für die Anforderungsauthentifizierung festgesetzt sind, führt ein IPSec-Authentifizierungsfehler zu einem wiederholten Verhalten, sodass die Kommunikation fortgesetzt werden kann, während die Authentifizierungsfehler untersucht werden.
- Die Anforderung, dass alle Geräte, die miteinander kommunizieren müssen, eine gemeinsame Reihe von Teilen:

- Authentifizierungsmethoden
- Hauptmodus-Schlüsselaustauschalgorithmen
- Daten Integritätsalgorithmen im Schnellmodus

  Wenn mindestens eine Gruppe von beiden Geräten nicht übereinstimmt, können die Geräte nicht erfolgreich kommuniziert werden.

Nachdem sich die Entwurfs-und Bereitstellungsteams auf diese Probleme geeinigt haben, können Sie die Bereitstellung des Windows Defender-Firewall-Designs fortsetzen. Weitere Informationen finden Sie unter Implementieren der Windows Defender-Firewall mit dem erweiterten Sicherheitsentwurfs Plan.

Implementieren Ihrer Windows Defender-Firewall mit erweitertem Sicherheitsentwurfs Plan

01.06.2019 • 2 minutes to read

Betrifft

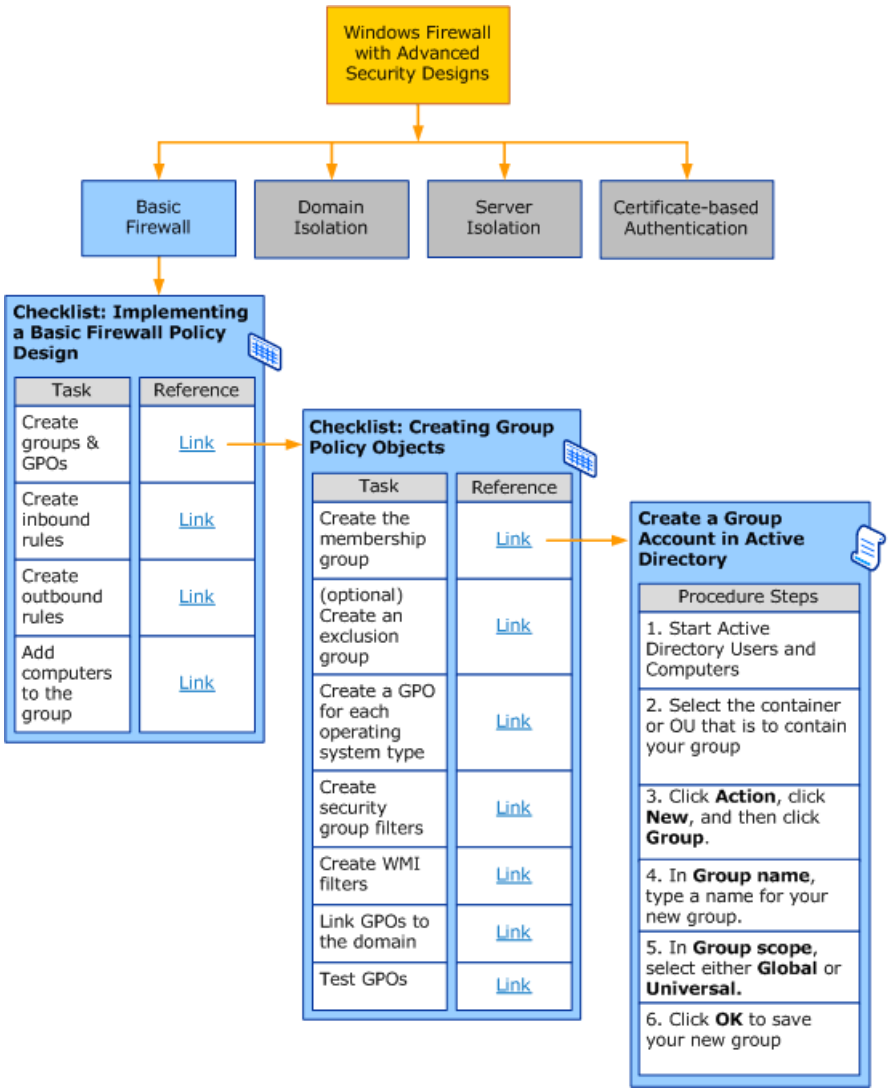
- Windows 10
- Windows Server 2016

Im folgenden sind wichtige Faktoren für die Implementierung des Entwurfsplans für die Windows Defender-Firewall zu finden:

- **Gruppenrichtlinie**. Die Windows Defender-Firewall mit erweiterten Sicherheitsdesigns nutzt die Gruppenrichtlinien, die von Active Directory-Domänendiensten (Adds) bereitgestellt werden. Zur erfolgreichen Bereitstellung der Firewall-und IPSec-Einstellungen und-Regeln für die Geräte in Ihrem Netzwerk ist eine Sound Gruppenrichtlinien-Infrastruktur erforderlich.
- **Umkreisfirewall**. Die meisten Organisationen verwenden eine Umkreisfirewall, um die Geräte im Netzwerk vor potenziell bösartigem Netzwerkdatenverkehr von außerhalb der Netzwerkgrenzen des Unternehmens zu schützen. Wenn Sie eine Bereitstellung planen, die eine Grenz Zone enthält, damit externe Geräte eine Verbindung mit Geräten in dieser Zone herstellen können, müssen Sie diesen Datenverkehr über die Umkreisfirewall auf die Geräte in der Grenz Zone zulassen.
- **Geräte, auf denen andere Betriebssysteme als Windows ausgeführt**werden. Wenn Ihr Netzwerkgeräte enthält, die nicht mit dem Windows-Betriebssystem ausgeführt werden, müssen Sie sicherstellen, dass die erforderliche Kommunikation mit diesen Geräten nicht durch die Einschränkungen blockiert wird, die durch Ihr Design auferlegt werden. Sie müssen eine der folgenden Aktionen ausführen:
  - Schließen Sie diese Geräte in die isolierte Domäne oder Zone ein, indem Sie Ihrem Entwurf eine zertifikatbasierte Authentifizierung hinzufügen. Viele andere Betriebssysteme können an einem isolierten Domänen-oder isolierten Server Szenario teilnehmen, sofern die zertifikatbasierte Authentifizierung verwendet wird.
  - Schließen Sie das Gerät in die in Ihrem Entwurf enthaltene Authentifizierungsausnahme Liste ein. Sie können diese Option auswählen, wenn das Gerät aus irgendeinem Grund nicht am Design der isolierten Domäne teilnehmen kann.

So implementieren Sie Ihre Windows Defender-Firewall mit erweitertem Sicherheitsdesign mithilfe dieses Leitfadens

Der nächste Schritt bei der Implementierung Ihres Entwurfs besteht darin, festzulegen, in welcher Reihenfolge die einzelnen Bereitstellungsschritte ausgeführt werden müssen. In diesem Leitfaden werden Prüflisten verwendet, die Ihnen helfen, die verschiedenen Bereitstellungsaufgaben zu erfüllen, die für die Implementierung Ihres Entwurfsplans erforderlich sind. Wie im folgenden Diagramm zu sehen ist, werden Checklisten und unter Prüflisten bei Bedarf verwendet, um das End-to-End-Verfahren für die Bereitstellungeines Entwurfs bereitzustellen.



Verwenden Sie die folgenden übergeordneten Checklisten in diesem Abschnitt des Leitfadens, um sich mit den Bereitstellungsaufgaben für die Implementierung der Windows Defender-Firewall Ihrer Organisation mit Advanced Security Design vertraut zu machen.

- Prüfliste: Implementieren des Entwurfs für eine allgemeine Firewallrichtlinie
- Prüfliste: Implementieren eines Entwurfs einer Domänenisolationsrichtlinie
- Prüfliste: Implementieren eines Entwurfs einer Domänenisolationsrichtlinie
- Prüfliste: Implementieren eines Entwurfs einer zertifikatbasierten Isolationsrichtlinie

Die Verfahren in diesen Checklisten verwenden die Gruppenrichtlinien-MMC-Snap-in-Schnittstellen, um Firewall- und Verbindungssicherheitsregeln in GPOs zu konfigurieren, Sie können aber auch Windows PowerShell verwenden. Weitere Informationen finden Sie unter Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell. Dieser Leitfaden empfiehlt die Verwendung von GPOs auf eine bestimmte Weise zum Bereitstellen der Regeln und Einstellungen für Ihren Entwurf. Informationen zum Bereitstellen von GPOs finden Sie unter Planen der Gruppenrichtlinienbereitstellung für Ihre Isolierungs Zonen und die Checkliste für die Checkliste : Erstellen von Gruppenrichtlinienobjekten.

Prüfliste: Erstellen von Gruppenrichtlinienobjekten

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Zum Bereitstellen von Firewall-oder IPSec-Einstellungen oder Firewall-oder Verbindungssicherheitsregeln empfiehlt es sich, die Gruppenrichtlinie in Adds zu verwenden. In diesem Abschnitt wird eine getestete, effiziente Methode beschrieben, die einige Voraussetzungen erfordert, aber einem Administrator langfristig zur Verdeutlichung dient, indem die Zuweisung von Gruppenrichtlinienobjekten so einfach wie das Löschen eines Geräts in eine Mitgliedschaftsgruppe ist.

Die Checklisten für Firewall, Domänenisolierung und Serverisolierung beinhalten einen Link zu dieser Checkliste.

Informationen zu Mitgliedschaftsgruppen

Bei den meisten Bereitstellungsaufgaben für Gruppenrichtlinienobjekte müssen Sie ermitteln, welche Geräte welche GPOs empfangen und anwenden müssen. Da unterschiedliche Versionen von Windows unterschiedliche Einstellungen und Regeln für ein ähnliches Verhalten unterstützen können, benötigen Sie möglicherweise mehrere Gruppenrichtlinienobjekte: eine für jedes Betriebssystem, deren Einstellungen sich von den anderen unterscheiden, um dasselbe Ergebnis zu erzielen. Beispielsweise verwenden Windows 10, Windows 8, Windows7, Windows Vista, Windows Server 2012, Windows Server2008 und Windows Server2008R2 Regeln und Einstellungen, die mit Windows 2000, WindowsXP und Windows Server2003 nicht kompatibel sind. Wenn in Ihrem Netzwerk die älteren Betriebssysteme enthalten sind, müssen Sie daher für jede Gruppe von Betriebssystemen, die allgemeine Einstellungen gemeinsam nutzen können, ein GPO erstellen. Zum Bereitstellen typischer Domänen Isolationseinstellungen und-Regeln sind möglicherweise fünf unterschiedliche GPOs für die in diesem Leitfaden besprochenen Windows-Versionen verfügbar. Wenn Sie die Verfahren in diesem Leitfaden befolgen, benötigen Sie nur eine Mitgliedschaftsgruppe, um alle fünf GPOs zu verwalten. Die Mitgliedschaftsgruppe ist im Sicherheitsgruppenfilter für alle fünf GPOs angegeben. Um die Einstellungen auf ein Gerät anzuwenden, stellen Sie das Konto des Geräts als Mitglied der Mitgliedschaftsgruppe ein. WMI-Filter werden verwendet, um sicherzustellen, dass das richtige Gruppenrichtlinienobjekt angewendet wird.

Informationen zu Ausschluss Gruppen

Bei einer Windows Defender-Firewall mit erweitertem Sicherheitsdesign müssen häufig Domänen verbundene Geräte im Netzwerk berücksichtigt werden, die die Regeln und Einstellungen in den GPOs nicht anwenden können oder dürfen. Da es sich bei diesen Geräten in der Regel um weniger als die Geräte handelt, die das Gruppenrichtlinienobjekt anwenden müssen, ist es einfacher, die Gruppe "Domänenmitglieder" in der Gruppe "GPO-Mitgliedschaft" zu verwenden und diese Ausnahme Geräte dann in einer Ausschlussgruppe zu platzieren, der die Anwendung von Gruppenrichtlinien verweigert wird. Berechtigungen für das Gruppenrichtlinienobjekt. Da DENY-Berechtigungen Vorrang vor Allow-Berechtigungen haben, wird ein Gerät, das Mitglied der Mitgliedschaftsgruppe und der Ausnahmegruppe ist, daran gehindert, das Gruppenrichtlinienobjekt anzuwenden. Zu den in der Ausschlussgruppe für Gruppenrichtlinienobjekte in der Regel für die Domänenisolierung gefundenen Geräten gehören die Domänencontroller, DHCP-Server und DNS-Server.

Sie können auch eine Mitgliedschaftsgruppe für eine Zone als Ausschlussgruppe für eine andere Zone verwenden. Beispielsweise sind Geräte in den Grenz-und Verschlüsselungs Zonen technisch im Hauptbereich der Domänenisolierung, müssen aber nur das Gruppenrichtlinienobjekt für die zugewiesene Rolle anwenden. Zu

diesem Zweck verweigern die GPOs für die Haupt Isolierungs Zone Gruppenrichtlinienberechtigungen für Mitglieder der Grenz-und Verschlüsselungs Zonen.

Checkliste: Erstellen von Gruppenrichtlinienobjekten

AUFGABE	REFERENZ
Überprüfen Sie wichtige Konzepte und Beispiele für die Bereitstellung von GPOs auf eine Weise, die den Anforderungen Ihrer Organisation am besten entspricht.	Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen Planen der Gruppenrichtlinienbereitstellung für die Netzwerkisolationszonen
Erstellen Sie die Mitgliedschaftsgruppe in Adds, die verwendet wird, um Geräte Konten zu enthalten, die das Gruppenrichtlinienobjekt empfangen müssen. Wenn auf einigen Geräten in der Gruppe Mitgliedschaft ein Betriebssystem ausgeführt wird, das keine WMI-Filter wie etwa Windows 2000 unterstützt, erstellen Sie eine Ausschlussgruppe, die die Geräte Konten für die Geräte enthält, die nicht mit einem WMI-Filter blockiert werden können.	Erstellen eines Gruppenkontos in Active Directory
Erstellen Sie für jede Windows-Version ein GPO mit unterschiedlichen Implementierungsanforderungen.	Erstellen eines Gruppenrichtlinienobjekts
Erstellen von Sicherheitsgruppen filtern, um das Gruppenrichtlinienobjekt auf Geräte zu beschränken, die Mitglieder der Mitgliedschaftsgruppe sind, und zum Ausschließen von Geräten, die Mitglieder der Ausschlussgruppe sind.	Zuweisen von Sicherheitsgruppenfiltern zum GPO
Erstellen Sie WMI-Filter, um jedes GPO auf die Geräte zu begrenzen, die den Kriterien im Filter entsprechen.	Erstellen von WMI-Filtern für Gruppenrichtlinienobjekte
Wenn Sie an einem GPO arbeiten, das von einem anderen kopiert wurde, ändern Sie die Gruppenmitgliedschaften und WMI-Filter so, dass Sie für die neue Zone oder Version von Windows, für die dieses GPO vorgesehen ist, korrekt sind.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Bevor Sie Regeln hinzufügen oder das Gruppenrichtlinienobjekt konfigurieren, fügen Sie der Gruppe Mitgliedschaft einige Testgeräte hinzu, und stellen Sie sicher, dass das richtige Gruppenrichtlinienobjekt empfangen und auf jedes Mitglied der Gruppe angewendet wird.	Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone

Prüfliste: Implementieren des Entwurfs für eine allgemeine Firewallrichtlinie

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese übergeordnete Checkliste enthält Querverweis Links zu wichtigen Konzepten des grundlegenden Firewall-Richtlinien Designs. Sie enthält außerdem Links zu untergeordneten Checklisten, die Ihnen bei der Durchführung der Aufgaben helfen, die zur Implementierung dieses Entwurfs erforderlich sind.

> **Hinweis:** führen Sie die Aufgaben in dieser Checkliste in der angegebenen Reihenfolge aus. Wenn ein Verweis Link Sie zu einer Prozedur führt, kehren Sie zu diesem Thema zurück, nachdem Sie die Schritte in diesem Verfahren ausgeführt haben, damit Sie die restlichen Aufgaben in dieser Checkliste fortsetzen können.

Die Verfahren in diesem Abschnitt verwenden die Gruppenrichtlinien-MMC-Snap-in-Schnittstellen, um die GPOs zu konfigurieren, Sie können aber auch Windows PowerShell verwenden. Weitere Informationen finden Sie unter Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell.

Prüfliste: Implementieren eines grundlegenden Firewall-Richtlinienentwurfs

AUFGABE	REFERENZ
Überprüfen Sie wichtige Konzepte und Beispiele für das grundlegende Firewall-Richtlinien Design, um festzustellen, ob dieses Design den Anforderungen Ihrer Organisation entspricht.	Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen Entwurf einer allgemeinen Firewallrichtlinie Beispiel für den Entwurf einer Firewallrichtlinie Planen der Einstellungen für eine allgemeine Firewallrichtlinie
Erstellen Sie die Mitgliedschaftsgruppe und ein GPO für jede Gruppe von Geräten, für die unterschiedliche Firewallregeln erforderlich sind. Wenn GPOs ähnlich sein sollen, beispielsweise für Windows 10 und Windows Server 2016, erstellen Sie ein GPO, konfigurieren Sie es mit den Aufgaben in dieser Checkliste, und erstellen Sie dann eine Kopie des Gruppenrichtlinienobjekts für die andere Version von Windows. Erstellen und konfigurieren Sie beispielsweise das GPO für Windows 10, erstellen Sie eine Kopie davon für Windows Server 2016, und führen Sie dann die Schritte in dieser Checkliste aus, um die wenigen erforderlichen Änderungen an der Kopie vorzunehmen.	Prüfliste: Erstellen von Gruppenrichtlinienobjekten Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
Wenn Sie an einem GPO arbeiten, das von einem anderen kopiert wurde, ändern Sie die Gruppenmitgliedschaft und die WMI-Filter so, dass Sie für die Geräte, für die dieses GPO vorgesehen ist, korrekt sind.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Konfigurieren Sie das Gruppenrichtlinienobjekt mit den Firewall-Standardeinstellungen, die für Ihren Entwurf geeignet sind.	Prüfliste: Konfigurieren von grundlegenden Firewalleinstellungen

AUFGABE	REFERENZ
Erstellen Sie mindestens eine eingehende Firewall-Regel, um unerwünschten eingehenden Netzwerkdatenverkehr zu ermöglichen.	Prüfliste: Erstellen von Eingangsfirewallregeln
Erstellen Sie mindestens eine ausgehende Firewall-Regel, um unerwünschten ausgehenden Netzwerkdatenverkehr zu blockieren.	Prüfliste: Erstellen von Ausgangsfirewallregeln
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Fügen Sie der Gruppe Mitgliedschaft Testgeräte hinzu, und überprüfen Sie dann, ob die Geräte die Firewallregeln wie erwartet von den GPOs empfangen.	Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone
Entsprechend dem Test-und Rollout Zeitplan in Ihrem Entwurfsplan fügen Sie der Gruppe "Mitgliedschaft" Geräte Konten hinzu, um die vollständigen Firewall-Richtlinieneinstellungen auf Ihren Geräten bereitzustellen.	Hinzufügen von Produktionsgeräten zur Mitgliedschaftsgruppe für eine Zone

Prüfliste: Konfigurieren von grundlegenden Firewalleinstellungen

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese Checkliste umfasst Aufgaben zum Konfigurieren eines GPO mit Firewall-Standardeinstellungen und Einstellungen, die von den Regeln getrennt sind.

Prüfliste: Konfigurieren von Standardeinstellungen und Einstellungen für Firewalls

AUFGABE	REFERENZ
Aktivieren Sie die Firewall, und setzen Sie das Standardverhalten für ein-und ausgehende Anrufe.	Aktivieren der Windows Defender-Firewall mit erweiterter Sicherheit und Konfigurieren des Standardverhaltens
Konfigurieren Sie die Firewall so, dass Benachrichtigungen für den Benutzer nicht angezeigt werden, wenn ein Programm blockiert ist, und um lokal definierte Firewall-und Verbindungssicherheitsregeln zu ignorieren.	Konfigurieren der Windows Defender-Firewall mit erweiterter Sicherheit, um Benachrichtigungen zu unterdrücken, wenn ein Programm blockiert wird
Konfigurieren Sie die Firewall so, dass eine Protokolldatei aufgezeichnet wird.	Konfigurieren der Windows Defender-Firewall mit erweitertem Sicherheitsprotokoll

Prüfliste: Erstellen von Eingangsfirewallregeln

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese Checkliste enthält Aufgaben zum Erstellen von Firewallregeln in Ihren GPOs.

Checkliste: Erstellen von Regeln für eingehende Firewalls

AUFGABE	REFERENZ
Erstellen Sie eine Regel, die es einem Programm ermöglicht, eingehenden Netzwerkdatenverkehr auf allen erforderlichen Ports zu überwachen und zu akzeptieren.	Erstellen einer Programm- oder Diensteingangsregel
Erstellen Sie eine Regel, die eingehenden Netzwerkdatenverkehr für eine angegebene Portnummer zulässt.	Erstellen einer Porteingangsregel
Erstellen Sie eine Regel, die eingehenden ICMP-Netzwerkdatenverkehr zulässt.	Erstellen einer ICMP-Eingangsregel
Erstellen Sie Regeln, die eingehenden RPC-Netzwerkdatenverkehr zulassen.	Erstellen von Eingangsregeln zur RPC-Unterstützung
Aktivieren einer vordefinierten Regel oder einer Gruppe vordefinierter Regeln Einige vordefinierte Regeln für grundlegende Netzwerkdienste sind im Rahmen der Installation von Windows enthalten; andere Personen können erstellt werden, wenn Sie eine neue Anwendung oder einen neuen Netzwerkdienst installieren.	Aktivieren von vordefinierten Eingangsregeln

Prüfliste: Erstellen von Ausgangsfirewallregeln

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese Checkliste enthält Aufgaben zum Erstellen von ausgehenden Firewallregeln in Ihren GPOs.

> **Wichtig:** standardmäßig ist die ausgehende Filterung deaktiviert. Da der gesamte ausgehende Netzwerkdatenverkehr zulässig ist, werden in der Regel ausgehende Regeln verwendet, um Datenverkehr zu blockieren, der im Netzwerk nicht erwünscht ist. Es ist jedoch eine bewährte Methode für einen Administrator, ausgehende Zulassungsregeln für diejenigen Anwendungen zu erstellen, die für die Verwendung im Netzwerk der Organisation genehmigt wurden. In diesem Fall haben Sie die Möglichkeit, das standardmäßige ausgehende Verhalten so festzulegen, dass Netzwerkdatenverkehr verhindert wird, der nicht ausdrücklich durch die von Ihnen erstellten Regeln autorisiert wurde.

Prüfliste: Erstellen von ausgehenden Firewallregeln für Windows 8, Windows 7, Windows Vista, Windows Server 2012, WindowsServer2008 oder Windows Server 2008 R2

AUFGABE	REFERENZ
Erstellen Sie eine Regel, die es einem Programm ermöglicht, ausgehenden Netzwerkdatenverkehr an einem beliebigen Port zu senden, der erforderlich ist.	Erstellen einer Programm- oder Dienstausgangsregel
Erstellen Sie eine Regel, die ausgehenden Netzwerkdatenverkehr für eine angegebene Portnummer zulässt.	Erstellen einer Portausgangsregel
Aktivieren einer vordefinierten Regel oder einer Gruppe vordefinierter Regeln Einige vordefinierte Regeln für grundlegende Netzwerkdienste sind im Rahmen der Installation von Windows enthalten; andere Personen können erstellt werden, wenn Sie eine neue Anwendung oder einen neuen Netzwerkdienst installieren.	Aktivieren von vordefinierten Ausgangsregeln

Prüfliste: Implementieren eines Entwurfs einer Domänenisolationsrichtlinie

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese übergeordnete Checkliste enthält Querverweis Links zu wichtigen Konzepten zum Domänen Isolierungs Richtlinienentwurf. Sie enthält außerdem Links zu untergeordneten Checklisten, die Ihnen bei der Durchführung der Aufgaben helfen, die zur Implementierung dieses Entwurfs erforderlich sind.

> **Hinweis:** führen Sie die Aufgaben in dieser Checkliste in der angegebenen Reihenfolge aus. Wenn ein Verweis Link Sie zu einer Prozedur führt, kehren Sie zu diesem Thema zurück, nachdem Sie die Schritte in diesem Verfahren ausgeführt haben, damit Sie die restlichen Aufgaben in dieser Checkliste fortsetzen können.

Die Verfahren in diesem Abschnitt verwenden die Gruppenrichtlinien-MMC-Snap-Ins zum Konfigurieren der GPOs, aber Sie können auch Windows PowerShell verwenden, um GPOs zu konfigurieren. Weitere Informationen finden Sie unter Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell.

Prüfliste: Implementieren eines Domänen Isolierungs Richtlinienentwurfs

AUFGABE	REFERENZ
Überprüfen Sie wichtige Konzepte und Beispiele für den Entwurf der Domänen Isolierungs Richtlinie, ermitteln Sie Ihre Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen, und passen Sie dieses Design an die Anforderungen Ihrer Organisation an.	Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen Entwurf einer Domänenisolationsrichtlinie Beispiel für den Entwurf einer Domänenisolationsrichtlinie Planen von Domänenisolationszonen
Erstellen Sie die GPOs und Verbindungssicherheitsregeln für die isolierte Domäne.	Prüfliste: Konfigurieren von Regeln für die isolierte Domäne
Erstellen Sie die GPOs und Verbindungssicherheitsregeln für die Grenz Zone.	Prüfliste: Konfigurieren von Regeln für die Begrenzungszone
Erstellen Sie die GPOs und Verbindungssicherheitsregeln für die Verschlüsselungszone.	Prüfliste: Konfigurieren von Regeln für die Verschlüsselungszone
Erstellen Sie die GPOs und Verbindungssicherheitsregeln für die isolierte Serverzone.	Prüfliste: Konfigurieren von Regeln für die Zone mit isolierten Servern
Fügen Sie gemäß dem Test-und Rollout Zeitplan Ihres Entwurfsplans Computerkonten zur Gruppe Mitgliedschaft hinzu, um Regeln und Einstellungen auf ihren Computern bereitzustellen.	Hinzufügen von Produktionsgeräten zur Mitgliedschaftsgruppe für eine Zone

AUFGABE	REFERENZ
Nachdem Sie bestätigt haben, dass der Netzwerkdatenverkehr durch IPSec authentifiziert wurde, können Sie die Authentifizierungsregeln für die isolierte Domäne und den Verschlüsselungsbereich von Anforderungs-in den require-Modus ändern.	Ändern des Regelmodus von Anforderung in Voraussetzung

Prüfliste: Konfigurieren von Regeln für die isolierte Domäne

07.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die folgenden Checklisten umfassen Aufgaben zum Konfigurieren von Verbindungssicherheitsregeln und IPSec-Einstellungen in Ihren GPOs, um die Haupt Zone in der isolierten Domäne zu implementieren.

Prüfliste: Konfigurieren von Regeln für isolierte Domänen

AUFGABE	REFERENZ
Erstellen Sie ein GPO für die Computer in der isolierten Domäne, auf der eines der Betriebssysteme ausgeführt wird. Nachdem Sie die Aufgaben in dieser Checkliste fertig gestellt und das Gruppenrichtlinienobjekt für diese Version von Windows konfiguriert haben, können Sie eine Kopie davon erstellen.	Prüfliste: Erstellen von Gruppenrichtlinienobjekten Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
Wenn Sie an einem GPO arbeiten, das aus einem anderen GPO kopiert wurde, ändern Sie die Gruppenmitgliedschaften und WMI-Filter so, dass Sie für die Zone der isolierten Domäne und die Version von Windows, für die dieses GPO vorgesehen ist, korrekt sind.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Konfigurieren Sie IPSec so, dass der gesamte ICMP-Netzwerkdatenverkehr vom IPSec-Schutz ausgenommen wird.	Ausschließen von ICMP aus der Authentifizierung
Erstellen Sie eine Regel, die den gesamten Netzwerkdatenverkehr von und zu Computern in der Ausnahmeliste von IPsec ausgenommen.	Erstellen einer Regel mit Authentifizierungsausnahmenliste
Konfigurieren Sie die zu verwendenden Sicherheitsmethoden und Algorithmen für den Schlüsselaustausch (Hauptmodus).	Konfigurieren von Einstellungen für den Schlüsselaustausch (Hauptmodus)
Konfigurieren Sie die zu verwendenden Algorithmus Kombinationen für den Datenschutz (Schnellmodus).	Konfigurieren von Einstellungen für den Datenschutz (Schnellmodus)
Konfigurieren Sie die zu verwendenden Authentifizierungsmethoden.	Konfigurieren von Authentifizierungsmethoden
Erstellen Sie die Regel, die die Authentifizierung für den gesamten eingehenden Netzwerkdatenverkehr anfordert.	Erstellen einer Authentifizierungsanforderungsregel
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der hinzugefügten Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne

AUFGABE	REFERENZ
Fügen Sie Ihre Testcomputer zur Mitgliedschaftsgruppe für die isolierte Domäne hinzu. Achten Sie darauf, mindestens eine für jedes Betriebssystem hinzuzufügen, das von einem anderen Gruppenrichtlinienobjekt in der Gruppe unterstützt wird.	Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone
Überprüfen Sie, ob die Verbindungssicherheitsregeln den Netzwerkdatenverkehr von und zu den Testcomputern schützen.	Sicherstellen, dass der Netzwerkdatenverkehr authentifiziert wird

Ändern Sie die Regeln für Ihre Zonen nicht so, dass eine Authentifizierung erforderlich ist, bis alle Zonen eingerichtet sind und ordnungsgemäß funktionieren.

Prüfliste: Konfigurieren von Regeln für die Begrenzungszone

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die folgenden Checklisten umfassen Aufgaben zum Konfigurieren von Verbindungssicherheitsregeln und IPSec-Einstellungen in Ihren GPOs, um die Grenz Zone in einer isolierten Domäne zu implementieren.

Regeln für die Grenz Zone sind in der Regel mit denen für die isolierte Domäne identisch, mit der Ausnahme, dass für die endgültige Regel nur die Authentifizierung angefordert, nicht erforderlich ist.

Prüfliste: Konfigurieren von Grenzzonen Regeln

In dieser Checkliste wird davon ausgegangen, dass Sie das Gruppenrichtlinienobjekt für die isolierte Domäne bereits erstellt haben, wie unter Checkliste: Implementieren eines Domänen Isolierungs Richtlinien Designsbeschrieben. Nachdem Sie eine Kopie für die Grenz Zone erstellt haben, stellen Sie sicher, dass Sie bei der Erstellung der anderen GPOs die Regel nicht von der Anforderungsauthentifizierung auf Authentifizierung anfordern ändern.

AUFGABE	REFERENZ
Erstellen Sie eine Kopie des Gruppenrichtlinienobjekts für die Domänenisolierung für diese Version von Windows, um als Ausgangspunkt für das Gruppenrichtlinienobjekt für die Grenz Zone zu fungieren. Im Gegensatz zum GPO für die Haupt Zone der isolierten Domäne wird diese Kopie nach der Bereitstellung nicht geändert, um eine Authentifizierung zu erfordern.	Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
Wenn Sie an einer Kopie eines GPO arbeiten, ändern Sie die Gruppenmitgliedschaften und WMI-Filter so, dass Sie für die Grenz Zone und die Version von Windows, für die dieses GPO vorgesehen ist, korrekt sind.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Fügen Sie Ihre Testcomputer zur Mitgliedschaftsgruppe für die Grenz Zone hinzu. Achten Sie darauf, mindestens eine für jedes Betriebssystem hinzuzufügen, das von einem anderen Gruppenrichtlinienobjekt in der Gruppe unterstützt wird.	Hinzufügen von Test Computern zur Mitgliedschaftsgruppe für eine Zone
Überprüfen Sie, ob die Verbindungs Sicherheitskonfiguration den Netzwerkdatenverkehr mit Authentifizierung schützt, wenn dies möglich ist, und dass nicht authentifizierter Datenverkehr akzeptiert wird.	Sicherstellen, dass der Netzwerkdatenverkehr authentifiziert wird

Prüfliste: Konfigurieren von Regeln für die Verschlüsselungszone

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese Checkliste umfasst Aufgaben zum Konfigurieren von Verbindungssicherheitsregeln und IPSec-Einstellungen in Ihren GPOs, um die Verschlüsselungszone in einer isolierten Domäne zu implementieren.

Regeln für die Verschlüsselungszone sind in der Regel mit denen für die isolierte Domäne identisch, mit der Ausnahme, dass die Hauptregel zusätzlich zur Authentifizierung eine Verschlüsselung erfordert.

Prüfliste: Konfigurieren von Verschlüsselungs Zonenregeln

In dieser Checkliste wird davon ausgegangen, dass Sie das Gruppenrichtlinienobjekt für die isolierte Domäne bereits erstellt haben, wie unter Checkliste: Implementieren eines Domänen Isolierungs Richtlinien Designsbeschrieben. Sie können diese GPOs dann kopieren, um Sie mit der Verschlüsselungszone zu verwenden. Nachdem Sie die Kopien erstellt haben, ändern Sie die Hauptregel, um zusätzlich zur Authentifizierung, die für die restliche isolierte Domäne erforderlich ist, eine Verschlüsselung vorzuschreiben.

AUFGABE	REFERENZ
Erstellen Sie eine Kopie der Domänen-Isolierungs-GPOs, um als Ausgangspunkt für die GPOs für die Verschlüsselungszone zu fungieren.	Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
Ändern Sie die Gruppenmitgliedschaften und WMI-Filter so, dass Sie für die Verschlüsselungszone und die Version von Windows, für die dieses GPO vorgesehen ist, korrekt sind.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Fügen Sie die Verschlüsselungsanforderungen für die Zone hinzu.	Konfigurieren der Regeln für eine zwingend erforderliche Verschlüsselung
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Fügen Sie Ihre Testcomputer zur Mitgliedschaftsgruppe für die Verschlüsselungszone hinzu. Achten Sie darauf, mindestens eine für jedes Betriebssystem hinzuzufügen, das von einem anderen Gruppenrichtlinienobjekt in der Gruppe unterstützt wird.	Hinzufügen von Test Computern zur Mitgliedschaftsgruppe für eine Zone
Überprüfen Sie, ob die Verbindungssicherheitsregeln den Netzwerkdatenverkehr schützen.	Sicherstellen, dass der Netzwerkdatenverkehr authentifiziert wird

Prüfliste: Konfigurieren von Regeln für die Zone mit isolierten Servern

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die folgenden Checklisten enthalten Aufgaben zum Konfigurieren von Verbindungssicherheitsregeln und IPSec-Einstellungen in Ihren GPOs für Server in einer isolierten Serverzone, die Teil einer isolierten Domäne sind. Informationen zum Erstellen einer eigenständigen isolierten Serverzone, die nicht Teil einer isolierten Domäne ist, finden Sie unter Checkliste: Implementieren eines eigenständigen Richtlinienentwurfs für die Serverisolierung.

Neben der Authentifizierung und der optionalen Verschlüsselung kann auf Server in einer isolierten Serverzone nur von Benutzern oder Geräten zugegriffen werden, die authentifizierte Mitglieder einer Netzwerkzugriffsgruppe (Network Access Group, NAG) sind. Wenn Sie Benutzerkonten in den nag einbeziehen, können die Einschränkungen weiterhin gelten. Sie werden nur auf der Anwendungsebene und nicht auf der IP-Ebene erzwungen.

Geräte, auf denen mindestens Windows Vista und Windows Server2008 ausgeführt werden, können sowohl Geräte als auch Benutzer im nag identifizieren, da IPSec in diesen Versionen von Windows zusätzlich zu IKE unterstützt AuthIP. AuthIP fügt Unterstützung für die benutzerbasierte Authentifizierung hinzu.

Die GPOs für einen isolierten Server oder eine Servergruppe ähneln denen für die isolierte Domäne selbst oder die Verschlüsselungszone, wenn Sie eine Verschlüsselung für Ihre isolierten Server benötigen. Diese Checkliste bezieht sich auf Verfahren zum Erstellen von Regeln sowie Einschränkungen, die es nur Mitgliedern des nag ermöglichen, eine Verbindung mit dem Server herzustellen.

Prüfliste: Konfigurieren von Regeln für isolierte Server

AUFGABE	REFERENZ
Erstellen Sie ein GPO für die Geräte, für die der Zugriff auf den gleichen Satz von Clientgeräten eingeschränkt sein muss. Wenn mehrere Server vorhanden sind und unterschiedliche Versionen des Windows-Betriebssystems ausgeführt werden, erstellen Sie zunächst das Gruppenrichtlinienobjekt für eine Windows-Version. Nachdem Sie die Aufgaben in dieser Checkliste fertig gestellt und das Gruppenrichtlinienobjekt für diese Version von Windows konfiguriert haben, können Sie eine Kopie davon erstellen. Kopieren Sie das Gruppenrichtlinienobjekt aus der isolierten Domäne oder aus der Verschlüsselungszone, um als Ausgangspunkt zu fungieren. Wenn Ihre Kopie bereits Elemente enthält, die in der folgenden Checkliste aufgeführt sind, überprüfen Sie die relevanten Verfahren, und vergleichen Sie diese mit dem Element des kopierten Gruppenrichtlinienobjekts, um sicherzustellen, dass es auf eine Weise konstruiert ist, die den Anforderungen der Server Isolations Zone entspricht.	Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts

AUFGABE	REFERENZ
Konfigurieren Sie die Sicherheitsgruppenfilter und WMI-Filter für das Gruppenrichtlinienobjekt, damit nur Mitglieder der Mitgliedschaftsgruppe der isolierten Serverzone, die die angegebene Version von Windows ausführt, Sie lesen und anwenden können.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Konfigurieren Sie IPSec so, dass der gesamte ICMP-Netzwerkdatenverkehr vom IPSec-Schutz ausgenommen wird.	Ausschließen von ICMP aus der Authentifizierung
Konfigurieren Sie die zu verwendenden Sicherheitsmethoden und Algorithmen für den Schlüsselaustausch (Hauptmodus).	Konfigurieren von Einstellungen für den Schlüsselaustausch (Hauptmodus)
Konfigurieren Sie die zu verwendenden Algorithmus Kombinationen für den Datenschutz (Schnellmodus). Wenn Sie für die isolierte Serverzone eine Verschlüsselung benötigen, stellen Sie sicher, dass Sie nur Algorithmus Kombinationen auswählen, die Verschlüsselung enthalten.	Konfigurieren von Einstellungen für den Datenschutz (Schnellmodus)
Konfigurieren Sie die zu verwendenden Authentifizierungsmethoden.	Konfigurieren von Authentifizierungsmethoden
Erstellen Sie eine Regel, die den gesamten Netzwerkdatenverkehr von und zu Geräten in der Ausnahmeliste von IPsec ausgenommen.	Erstellen einer Regel mit Authentifizierungsausnahmenliste
Erstellen Sie eine Regel, die die Authentifizierung für den gesamten Netzwerkdatenverkehr anfordert. **Wichtig:** Legen Sie wie in einer isolierten Domäne die Regeln nicht so fest, dass für eingehenden Datenverkehr eine Authentifizierung erforderlich ist, bis Sie die Tests abgeschlossen haben. Wenn die Regeln nicht erwartungsgemäß funktionieren, sind die Kommunikationen auf diese Weise nicht von einem Fehler bei der Authentifizierung betroffen.	Erstellen einer Authentifizierungsanforderungsregel
Erstellen Sie das nag-Element, das die Geräte-oder Benutzerkonten enthält, die auf die Server in der Zone des isolierten Servers zugreifen dürfen.	Erstellen eines Gruppenkontos in Active Directory
Erstellen Sie eine Firewall-Regel, die eingehenden Netzwerkdatenverkehr nur dann zulässt, wenn Sie als Mitglied des nag authentifiziert sind.	Einschränken des Serverzugriffs auf Mitglieder einer Gruppe
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Fügen Sie den Testserver zur Mitgliedschaftsgruppe für die isolierte Serverzone hinzu. Stellen Sie sicher, dass mindestens ein Server für jedes Betriebssystem hinzugefügt wird, das von einem Gruppenrichtlinienobjekt in der Gruppe unterstützt wird.	Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone

Ändern Sie die Regeln für Ihre Zonen nicht so, dass eine Authentifizierung erforderlich ist, bis alle Zonen eingerichtet sind und ordnungsgemäß funktionieren.

Prüfliste: Implementieren eines eigenständigen Entwurfs einer Serverisolationsrichtlinie

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese Checkliste enthält Verfahren zum Erstellen eines Server Isolierungs Richtlinien Designs, das nicht Bestandteileiner isolierten Domäne ist. Die erforderlichen Schritte zum Erstellen einer isolierten Serverzone innerhalb einer isolierten Domäne finden Sie unter Checkliste: Konfigurieren von Regeln für eine isolierte Serverzone.

Diese übergeordnete Checkliste enthält Querverweis Links zu wichtigen Konzepten zum Domänen Isolierungs Richtlinienentwurf. Sie enthält außerdem Links zu untergeordneten Checklisten, die Ihnen bei der Durchführung der Aufgaben helfen, die zur Implementierung dieses Entwurfs erforderlich sind.

> **Hinweis:** führen Sie die Aufgaben in dieser Checkliste in der angegebenen Reihenfolge aus. Wenn ein Verweis Link Sie zu einer Prozedur führt, kehren Sie zu diesem Thema zurück, nachdem Sie die Schritte in diesem Verfahren ausgeführt haben, damit Sie die restlichen Aufgaben in dieser Checkliste fortsetzen können.

Prüfliste: Implementieren eines eigenständigen Richtlinienentwurfs für die Serverisolierung

AUFGABE	REFERENZ
Überprüfen Sie wichtige Konzepte und Beispiele für den Entwurf der Server Isolierungs Richtlinie, um festzustellen, ob dieser Entwurf ihre Bereitstellungsziele und die Anforderungen Ihrer Organisation erfüllt.	Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen Entwurf einer Serverisolationsrichtlinie Beispiel für den Entwurf einer Serverisolationsrichtlinie Planen von Serverisolationszonen
Erstellen Sie die GPOs und Verbindungssicherheitsregeln für isolierte Server.	Prüfliste: Konfigurieren von Regeln für Server in einer eigenständigen Zone mit isolierten Servern
Erstellen Sie die GPOs und Verbindungssicherheitsregeln für die Clientgeräte, die mit den isolierten Servern verbunden werden müssen.	Prüfliste: Erstellen von Regeln für Clients einer eigenständigen Zone mit isolierten Servern
Überprüfen Sie, ob die Verbindungssicherheitsregeln den Netzwerkdatenverkehr auf Ihren Testgeräten schützen.	Sicherstellen, dass der Netzwerkdatenverkehr authentifiziert wird
Nachdem Sie bestätigt haben, dass der Netzwerkdatenverkehr wie erwartet von IPSec authentifiziert wurde, können Sie die Authentifizierungsregeln für die isolierte Serverzone so ändern, dass eine Authentifizierung erforderlich ist, anstatt sie anzufordern.	Ändern des Regelmodus von Anforderung in Voraussetzung
Entsprechend dem Test-und Rollout Zeitplan in Ihrem Entwurfsplan fügen Sie der Gruppe Mitgliedschaft Geräte Konten für die Clientgeräte hinzu, damit Sie die Einstellungen bereitstellen können.	Hinzufügen von Produktionsgeräten zur Mitgliedschaftsgruppe für eine Zone

AUFGABE	REFERENZ

Prüfliste: Konfigurieren von Regeln für Server in einer eigenständigen Zone mit isolierten Servern

07.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese Checkliste umfasst Aufgaben zum Konfigurieren von Verbindungssicherheitsregeln und IPSec-Einstellungen in Ihren GPOs für Server in einer eigenständigen isolierten Serverzone, die nicht Teil einer isolierten Domäne ist. Neben der Authentifizierung und der optionalen Verschlüsselung sind Server in einer Server Isolations Zone nur von Benutzern oder Geräten zugänglich, die als Mitglieder einer Netzwerkzugriffsgruppe (Network Access Group, NAG) authentifiziert sind. Die hier beschriebenen GPOs gelten nur für die isolierten Server, nicht für die Clientgeräte, die mit Ihnen verbunden sind. Informationen zu den GPOs für die Clientgeräte finden Sie unter Checkliste: Erstellen von Regeln für Clients einer eigenständigen isolierten Server Zone.

Die GPOs für isolierte Server ähneln denen für eine isolierte Domäne. Diese Checkliste verweist auf die Verfahren für die Erstellung einiger Regeln. Die anderen Verfahren in dieser Checkliste dienen zum Erstellen von Einschränkungen, mit denen nur Mitglieder der Serverzugriffs Gruppe eine Verbindung mit dem Server herstellen können.

Prüfliste: Konfigurieren von Regeln für isolierte Server

AUFGABE	REFERENZ
Erstellen Sie ein GPO für die Geräte, für die der Zugriff auf den gleichen Satz von Clientgeräten eingeschränkt sein muss. Wenn mehrere Server mit unterschiedlichen Versionen des Windows-Betriebssystems ausgeführt werden, erstellen Sie zunächst das Gruppenrichtlinienobjekt für eine Windows-Version. Nachdem Sie die Aufgaben in dieser Checkliste fertig gestellt und das Gruppenrichtlinienobjekt für diese Version von Windows konfiguriert haben, können Sie eine Kopie davon erstellen.	Prüfliste: Erstellen von Gruppenrichtlinienobjekten Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
Wenn Sie an einer Kopie eines GPO arbeiten, ändern Sie die Gruppenmitgliedschaften und WMI-Filter so, dass Sie für die Geräte, für die dieses GPO vorgesehen ist, korrekt sind.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Konfigurieren Sie IPSec so, dass der gesamte ICMP-Netzwerkdatenverkehr vom IPSec-Schutz ausgenommen wird.	Ausschließen von ICMP aus der Authentifizierung
Erstellen Sie eine Regel, die den gesamten Netzwerkdatenverkehr von und zu Geräten in der Ausnahmeliste von IPsec ausgenommen.	Erstellen einer Regel mit Authentifizierungsausnahmenliste
Konfigurieren Sie die zu verwendenden Sicherheitsmethoden und Algorithmen für den Schlüsselaustausch (Hauptmodus).	Konfigurieren von Einstellungen für den Schlüsselaustausch (Hauptmodus)
Konfigurieren Sie die zu verwendenden Algorithmus Kombinationen für den Datenschutz (Schnellmodus).	Konfigurieren von Einstellungen für den Datenschutz (Schnellmodus)

AUFGABE	REFERENZ
Konfigurieren Sie die zu verwendenden Authentifizierungsmethoden. Dieses Verfahren legt die Standardeinstellungen für das Gerät fest. Diese Vorgehensweise ist optional, wenn Sie die Authentifizierung für jede Regel einrichten möchten.	Konfigurieren von Authentifizierungsmethoden
Erstellen Sie eine Regel, die die Authentifizierung für den gesamten eingehenden Netzwerkdatenverkehr anfordert. **Wichtig:** Legen Sie genauso wie in einer isolierten Domäne die Regeln nicht so fest, dass eine Authentifizierung erforderlich ist, bis die Tests abgeschlossen sind. Wenn die Regeln nicht erwartungsgemäß funktionieren, sind die Kommunikationen auf diese Weise nicht von einem Fehler bei der Authentifizierung betroffen.	Erstellen einer Authentifizierungsanforderungsregel
Wenn für Ihr Design zusätzlich zur Authentifizierung für den Zugriff auf die isolierten Server eine Verschlüsselung erforderlich ist, müssen Sie die Regel so ändern, dass Sie erforderlich ist.	Konfigurieren der Regeln für eine zwingend erforderliche Verschlüsselung
Erstellen Sie das nag-Element, das die Geräte-oder Benutzerkonten enthält, die auf die isolierten Server zugreifen dürfen. Wenn Sie über mehrere Gruppen von isolierten Servern verfügen, auf die von verschiedenen Clientgeräten zugegriffen wird, erstellen Sie einen NAG für jede Gruppe von Servern.	Erstellen eines Gruppenkontos in Active Directory
Erstellen Sie eine Firewallregel, die eingehenden Netzwerkdatenverkehr nur dann zulässt, wenn Sie von einem Benutzer oder Gerät authentifiziert wird, das Mitglied des nag der Zone ist.	Einschränken des Serverzugriffs auf Mitglieder einer Gruppe
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Fügen Sie den Testserver zur Mitgliedschaftsgruppe für die isolierte Serverzone hinzu. Achten Sie darauf, mindestens eine für jedes Betriebssystem hinzuzufügen, das von einem anderen Gruppenrichtlinienobjekt in der Gruppe unterstützt wird.	Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone

Ändern Sie die Regeln für Ihre Zonen nicht so, dass eine Authentifizierung erforderlich ist, bis alle Zonen eingerichtet und gründlich getestet wurden.

Prüfliste: Erstellen von Regeln für Clients einer eigenständigen Zone mit isolierten Servern

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Diese Checkliste umfasst Aufgaben zum Konfigurieren von Verbindungssicherheitsregeln und IPSec-Einstellungen in den GPOs für Clientgeräte, die eine Verbindung mit Servern in einer isolierten Serverzone herstellen müssen.

Prüfliste: Konfigurieren von Clientregeln für isolierte Server Zonen

AUFGABE	REFERENZ
Erstellen Sie ein GPO für die Clientgeräte, die eine Verbindung mit Servern in der Zone des isolierten Servers herstellen müssen und auf denen eine der Versionen von Windows ausgeführt wird. Nachdem Sie die Aufgaben in dieser Checkliste fertig gestellt haben, können Sie eine Kopie davon erstellen.	Prüfliste: Erstellen von Gruppenrichtlinienobjekten Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
Wenn Sie feststellen möchten, welche Geräte das Gruppenrichtlinienobjekt empfangen, weisen Sie den NAG für die isolierten Server dem Sicherheitsgruppenfilter für das Gruppenrichtlinienobjekt zu. Stellen Sie sicher, dass die einzelnen Gruppenrichtlinienobjekte über den WMI-Filter für die richtige Windows-Version verfügen.	Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
Konfigurieren Sie IPSec so, dass der gesamte ICMP-Netzwerkdatenverkehr vom IPSec-Schutz ausgenommen wird.	Ausschließen von ICMP aus der Authentifizierung
Erstellen Sie eine Regel, die den gesamten Netzwerkdatenverkehr von und zu Geräten in der Ausnahmeliste von IPsec ausgenommen.	Erstellen einer Regel mit Authentifizierungsausnahmenliste
Konfigurieren Sie die zu verwendenden Sicherheitsmethoden und Algorithmen für den Schlüsselaustausch (Hauptmodus).	Konfigurieren von Einstellungen für den Schlüsselaustausch (Hauptmodus)
Konfigurieren Sie die zu verwendenden Algorithmus Kombinationen für den Datenschutz (Schnellmodus).	Konfigurieren von Einstellungen für den Datenschutz (Schnellmodus)
Konfigurieren Sie die zu verwendenden Authentifizierungsmethoden.	Konfigurieren von Authentifizierungsmethoden

AUFGABE	REFERENZ
Erstellen Sie eine Regel, die die Authentifizierung für den Netzwerkdatenverkehr anfordert. Da das Fall Back-to-Clear-Verhalten in Windows Vista und Windows Server2008 keine Verzögerungen bei der Kommunikation mit Geräten hat, die IPSec nicht verwenden können, können Sie dieselbe Any-to-any-Regel verwenden, die in einer isolierten Domäne verwendet wird.	Erstellen einer Authentifizierungsanforderungsregel
Verknüpfen Sie das Gruppenrichtlinienobjekt mit der Domänenebene der Active Directory-Organisationseinheitshierarchie.	Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
Fügen Sie die Testgeräte zum NAG für die Zone des isolierten Servers hinzu. Achten Sie darauf, mindestens eine für jedes Betriebssystem hinzuzufügen, das von einem anderen Gruppenrichtlinienobjekt in der Gruppe unterstützt wird.	Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone

Prüfliste: Implementieren eines Entwurfs einer zertifikatbasierten Isolationsrichtlinie

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Diese übergeordnete Checkliste enthält Querverweis Links zu wichtigen Konzepten zur Verwendung von Zertifikaten als Authentifizierungsoption in einer Domänenisolierung oder einem Server Isolierungs Entwurf.

> **Hinweis:** führen Sie die Aufgaben in dieser Checkliste in der angegebenen Reihenfolge aus. Wenn ein Verweis Link Sie zu einer Prozedur führt, kehren Sie zu diesem Thema zurück, nachdem Sie die Schritte in diesem Verfahren ausgeführt haben, damit Sie die restlichen Aufgaben in dieser Checkliste fortsetzen können.

Prüfliste: Implementieren der zertifikatbasierten Authentifizierung

AUFGABE	REFERENZ
Überprüfen Sie wichtige Konzepte und Beispiele für die zertifikatbasierte Authentifizierung, um festzustellen, ob dieses Design ihre Bereitstellungsziele und die Anforderungen Ihrer Organisation erfüllt.	Identifizieren der Windows Defender-Firewall mit erweiterten Sicherheits Bereitstellungszielen Entwurf einer zertifikatbasierten Isolationsrichtlinie Beispiel für den Entwurf einer zertifikatbasierten Isolationsrichtlinie Planen der zertifikatbasierten Authentifizierung
Installieren Sie die Rolle "Active Directory Certificate Services (MDE)" als Zertifizierungsstelle für die Unternehmensstammzertifizierungsstelle. Dieser Schritt ist nur erforderlich, wenn Sie in Ihrem Netzwerk noch keine Zertifizierungsstelle bereitgestellt haben.	
Konfigurieren Sie die Zertifikatvorlage für Workstation-Authentifizierungszertifikate.	Konfigurieren der Zertifikatvorlage zur Arbeitsstationsauthentifizierung
Konfigurieren Sie Gruppenrichtlinien so, dass Zertifikate basierend auf Ihrer Vorlage automatisch auf Workstation-Geräten bereitgestellt werden.	Konfigurieren der Gruppenrichtlinie für die automatische Registrierung und für die Bereitstellung von Zertifikaten
Aktualisieren Sie auf einem Testgerät Gruppenrichtlinien, und bestätigen Sie, dass das Zertifikat installiert ist.	Bestätigen, dass Zertifikate ordnungsgemäß bereitgestellt werden

In dieser Anleitung verwendete Vorgehensweisen

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die Verfahren in diesem Abschnitt werden in den zuvor in diesem Dokument gefundenen Checklisten angezeigt. Sie sollten nur im Kontext der Checklisten verwendet werden, in denen Sie angezeigt werden. Sie werden hier in alphabetischer Reihenfolge angezeigt.

- Hinzufügen von Produktionsgeräten zur Mitgliedschaftsgruppe für eine Zone
- Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone
- Zuweisen von Sicherheitsgruppenfiltern zum GPO
- Ändern des Regelmodus von Anforderung in Voraussetzung
- Konfigurieren von Authentifizierungsmethoden
- Konfigurieren von Einstellungen für den Datenschutz (Schnellmodus)
- Konfigurieren der Gruppenrichtlinie für die automatische Registrierung und für die Bereitstellung von Zertifikaten
- Konfigurieren von Einstellungen für den Schlüsselaustausch (Hauptmodus)
- Konfigurieren der Regeln für eine zwingend erforderliche Verschlüsselung
- Konfigurieren der Windows Defender-Firewall mit erweitertem Sicherheitsprotokoll
- Konfigurieren der Zertifikatvorlage zur Arbeitsstationsauthentifizierung
- Konfigurieren der Windows Defender-Firewall mit erweiterter Sicherheit, um Benachrichtigungen zu unterdrücken, wenn ein Programm blockiert wird
- Bestätigen, dass Zertifikate ordnungsgemäß bereitgestellt werden
- Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts
- Erstellen eines Gruppenkontos in Active Directory
- Erstellen eines Gruppenrichtlinienobjekts
- Erstellen einer Regel mit Authentifizierungsausnahmenliste
- Erstellen einer Authentifizierungsanforderungsregel
- Erstellen einer ICMP-Eingangsregel
- Erstellen einer Porteingangsregel
- Erstellen einer Programm- oder Diensteingangsregel
- Erstellen einer Portausgangsregel
- Erstellen einer Programm- oder Dienstausgangsregel

- Erstellen von Eingangsregeln zur RPC-Unterstützung
- Erstellen von WMI-Filtern für Gruppenrichtlinienobjekte
- Aktivieren von vordefinierten Eingangsregeln
- Aktivieren von vordefinierten Ausgangsregeln
- Ausschließen von ICMP aus der Authentifizierung
- Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne
- Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows
- Öffnen der Gruppenrichtlinien-Verwaltungskonsole zu IP-Sicherheitsrichtlinien
- Öffnen der Gruppenrichtlinien-Verwaltungskonsole für die Windows Defender-Firewall mit erweiterter Sicherheit
- Öffnen der Windows Defender-Firewall mit erweiterter Sicherheit
- Einschränken des Serverzugriffs auf Mitglieder einer Gruppe
- Aktivieren der Windows Defender-Firewall mit erweiterter Sicherheit und Konfigurieren des Standardverhaltens
- Sicherstellen, dass der Netzwerkdatenverkehr authentifiziert wird

Hinzufügen von Produktionsgeräten zur Mitgliedschaftsgruppe für eine Zone

10.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie die GPOs für Ihren Entwurf auf einem kleinen Satz von Geräten getestet haben, können Sie diese auf den Produktionsgeräten bereitstellen.

Vorsicht bei GPOs, die Verbindungssicherheitsregeln enthalten, die nicht authentifizierte Verbindungen verhindern, stellen Sie sicher, dass Sie während der Testphase die Regeln so festlegen, dass die Authentifizierung angefordert und nicht erforderlich ist. Nachdem Sie das Gruppenrichtlinienobjekt bereitgestellt und bestätigt haben, dass alle Ihre Geräte erfolgreich mithilfe von authentifiziertem IPSec kommunizieren, können Sie das Gruppenrichtlinienobjekt so ändern, dass eine Authentifizierung erforderlich ist. Ändern Sie das Gruppenrichtlinienobjekt für Grenzzonen nicht in den Modus erforderlich.

Die in diesem Leitfaden beschriebene Methode verwendet die integrierte Gruppe " **Domänencomputer** ". Der Vorteil dieser Methode besteht darin, dass alle neuen Geräte, die der Domäne angehören, automatisch das GPO der isolierten Domäne empfangen. Um dies erfolgreich durchführen zu können, müssen Sie sicherstellen, dass die WMI-Filter und die Sicherheitsgruppe Filtergeräte ausschließen, die die GPOs nicht empfangen dürfen. Verwenden Sie Gerätegruppen, die sowohl Lese-als auch Gruppenrichtlinienberechtigungen für die GPOs verweigern, beispielsweise eine im CG_DOMISO_NOIPSEC-Beispiel Entwurf verwendete Gruppe. Geräte, die Mitglieder einiger Zonen sind, müssen auch von der Anwendung der GPOs für die Haupt isolierte Domäne ausgeschlossen werden. Weitere Informationen finden Sie im Abschnitt "verhindern, dass Mitglieder einer Gruppe ein GPO anwenden" unter Zuweisen von Sicherheitsgruppen Filtern zum Gruppenrichtlinienobjekt.

Ohne eine solche Gruppe (oder Gruppen) müssen Sie entweder Geräte einzeln hinzufügen oder die Gruppen mit Geräte Konten verwenden, die Ihnen zur Verfügung stehen.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder über eine anderweitige Berechtigung verfügen, um die Mitgliedschaft der Gruppe für das Gruppenrichtlinienobjekt zu ändern.

In diesem Thema:

So fügen Sie der Gruppenrichtlinien-Mitgliedschaftsgruppe Domänen Geräte hinzu

1. Öffnen Sie Active Directory-Benutzer und -Computer.
2. Erweitern Sie im Navigationsbereich **Active Directory-Benutzer und-Computer**, erweitern Sie *IhrDomänenname*und dann den Container, in dem Sie die Mitgliedschaftsgruppe erstellt haben.

3. Doppelklicken Sie im Detailbereich auf die Gruppenrichtlinien-Mitgliedschaftsgruppe, der Sie Computer hinzufügen möchten.
4. Wählen Sie die Registerkarte **Mitglieder** aus, und klicken Sie dann auf **Hinzufügen**.
5. Geben Sie im Textfeld **Domänencomputer** ein, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **OK** , um das Dialogfeld Gruppeneigenschaften zu schließen.

Nachdem ein Computer ein Mitglied der Gruppe ist, können Sie eine Gruppenrichtlinienaktualisierung auf dem Computer erzwingen.

So aktualisieren Sie die Gruppenrichtlinie auf einem Gerät

Geben Sie an einer Eingabeaufforderung mit erhöhten Rechten Folgendes ein:

```
gpupdate /target:computer /force
```

Nachdem die Gruppenrichtlinie aktualisiert wurde, können Sie sehen, welche GPOs aktuell auf den Computer angewendet werden.

So stellen Sie fest, welche GPOs auf ein Gerät angewendet werden

Geben Sie an einer Eingabeaufforderung mit erhöhten Rechten Folgendes ein:

```
gpresult /r /scope:computer
```

Hinzufügen von Testgeräten zur Mitgliedschaftsgruppe für eine Zone

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Bevor Sie Ihre Regeln für eine große Anzahl von Geräten bereitstellen, müssen Sie die Regeln gründlich testen, um sicherzustellen, dass die Kommunikation wie erwartet funktioniert. Ein falsch eingegebener WMI-Filter oder eine falsch typisierte IP-Adresse in einer Filterliste kann die Kommunikation zwischen Geräten problemlos blockieren. Obwohl es empfehlenswert ist, ihre Regeln auf den Anforderungsmodus festzulegen, bis die Prüfung und Bereitstellung abgeschlossen ist, empfehlen wir, dass Sie die Regeln zunächst nur auf einer kleinen Anzahl von Geräten bereitstellen, um sicherzustellen, dass die richtigen GPOs von jedem Gerät verarbeitet werden.

Fügen Sie jeder Mitgliedschaftsgruppe mindestens ein Gerät jedes unterstützten Betriebssystemtyps hinzu. Stellen Sie sicher, dass jedes GPO für eine bestimmte Version von Windows und die Mitgliedschaftsgruppe über ein Gerät in der Testgruppe verfügt. Nachdem die Gruppenrichtlinien auf jedem Testgerät aktualisiert wurden, überprüfen Sie die Ausgabe des Befehls **gpresult** , um zu bestätigen, dass jedes Gerät nur die Gruppenrichtlinienobjekte empfängt, die es erhalten soll.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder über eine anderweitige Berechtigung verfügen, um die Mitgliedschaft der Gruppe für das Gruppenrichtlinienobjekt zu ändern.

In diesem Thema:

So fügen Sie Testgeräte zu Mitgliedschaftsgruppen für Gruppenrichtlinienobjekte hinzu

1. Öffnen Sie Active Directory-Benutzer und -Computer.
2. Erweitern Sie im Navigationsbereich **Active Directory-Benutzer und-Computer**, erweitern Sie *IhrDomänenname*, und erweitern Sie dann den Container, in dem Ihr Mitgliedschaftsgruppen Konto gespeichert ist.
3. Doppelklicken Sie im Detailbereich auf die Gruppenrichtlinien-Mitgliedschaftsgruppe, der Sie Geräte hinzufügen möchten.
4. Wählen Sie die Registerkarte **Mitglieder** aus, und klicken Sie dann auf **Hinzufügen**.
5. Geben Sie den Namen des Geräts in das Textfeld ein, und klicken Sie dann auf **OK**.
6. Wiederholen Sie die Schritte 5 und 6 für jedes zusätzliche Geräte Konto oder jede weitere Gruppe, die Sie

hinzufügen möchten.

7. Klicken Sie auf **OK** , um das Dialogfeld Gruppeneigenschaften zu schließen.

Nachdem ein Gerät ein Mitglied der Gruppe ist, können Sie eine Gruppenrichtlinienaktualisierung auf dem Gerät erzwingen.

So aktualisieren Sie die Gruppenrichtlinie auf einem Gerät

Führen Sie an einer Eingabeaufforderung mit erhöhten Rechten die folgenden Aktionen aus:

```
gpupdate /target:device /force
```

Nachdem die Gruppenrichtlinie aktualisiert wurde, können Sie sehen, welche GPOs aktuell auf das Gerät angewendet werden.

So stellen Sie fest, welche GPOs auf ein Gerät angewendet werden

Führen Sie an einer Eingabeaufforderung mit erhöhten Rechten die folgenden Aktionen aus:

```
gpresult /r /scope:computer
```

Zuweisen von Sicherheitsgruppenfiltern zum GPO

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie sicherstellen möchten, dass Ihr Gruppenrichtlinienobjekt auf die richtigen Computer angewendet wird, verwenden Sie das MMC-Snap-in Gruppenrichtlinienverwaltung, um dem Gruppenrichtlinienobjekt Sicherheitsgruppenfilter zuzuweisen.

> **IMPORTANT**
> Dieser Bereitstellungsleitfaden verwendet die Methode zum Hinzufügen der Gruppe "Domänencomputer" zur Mitgliedschaftsgruppe für die Haupt isolierte Domäne, nachdem die Tests abgeschlossen sind und Sie bereit sind, in die Produktion zu wechseln. Damit diese Methode funktioniert, müssen Sie verhindern, dass jeder Computer, der Mitglied der Grenz-oder Verschlüsselungszone ist, das Gruppenrichtlinienobjekt für die Haupt isolierte Domäne anwendet. Verweigern Sie beispielsweise für die GPOs für die Haupt isolierte Domäne die Berechtigung Lesen und Gruppenrichtlinienberechtigungen für die Mitgliedschaftsgruppen für die Grenz-und Verschlüsselungs Zonen.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der relevanten GPOs verfügen.

In diesem Thema:

So ermöglichen Sie Mitgliedern einer Gruppe das Anwenden eines Gruppenrichtlinienobjekts

Gehen Sie wie folgt vor, um dem Sicherheitsfilter für das Gruppenrichtlinienobjekt eine Gruppe hinzuzufügen, die es Gruppenmitgliedern ermöglicht, das Gruppenrichtlinienobjekt anzuwenden.

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Suchen Sie im Navigationsbereich, und klicken Sie dann auf das Gruppenrichtlinienobjekt, das Sie ändern möchten.
3. Klicken Sie im Detailbereich unter **Sicherheitsfilterung**auf **Authentifizierte Benutzer**, und klicken Sie dann auf **Entfernen**.

> **NOTE**
>
> Sie müssen die Standardberechtigung, die allen authentifizierten Benutzern und Computern gewährt wurde, entfernen, um das Gruppenrichtlinienobjekt auf die von Ihnen angegebenen Gruppen zu beschränken. Wenn das Gruppenrichtlinienobjekt Benutzereinstellungen enthält und die Gruppe **Authentifizierte Benutzer** entfernt wird und eine neue Sicherheitsfilterung mithilfe einer Sicherheitsgruppe hinzugefügt wird, die nur Benutzerkonten enthält, kann das Gruppenrichtlinienobjekt nicht angewendet werden. Details und verschiedene Problemumgehungen werden in diesem Microsoft-Blogerwähnt.

4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppe auswählen** den Namen der Gruppe ein, deren Mitglieder das Gruppenrichtlinienobjekt anwenden sollen, und klicken Sie dann auf **OK**. Wenn Sie den Namen nicht kennen, können Sie auf **erweitert** klicken, um die Liste der in der Domäne verfügbaren Gruppen zu durchsuchen.

So verhindern Sie, dass Mitglieder einer Gruppe ein Gruppenrichtlinienobjekt anwenden

Gehen Sie wie folgt vor, um dem Sicherheitsfilter für das Gruppenrichtlinienobjekt eine Gruppe hinzuzufügen, die verhindert, dass Gruppenmitglieder das Gruppenrichtlinienobjekt anwenden. Dies wird in der Regel verwendet, um zu verhindern, dass Mitglieder der Grenz-und Verschlüsselungs Zonen die GPOs für die isolierte Domäne anwenden.

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Suchen Sie im Navigationsbereich, und klicken Sie dann auf das Gruppenrichtlinienobjekt, das Sie ändern möchten.
3. Klicken Sie im Detailbereich auf die **** Registerkarte Delegierung.
4. Klicken Sie auf **Erweitert**.
5. Klicken Sie unter der Liste **Gruppen-oder Benutzernamen** auf **Hinzufügen**.
6. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppe auswählen** den Namen der Gruppe ein, deren Mitglieder daran gehindert werden sollen, das Gruppenrichtlinienobjekt anzuwenden, und klicken Sie dann auf **OK**. Wenn Sie den Namen nicht kennen, können Sie auf **erweitert** klicken, um die Liste der in der Domäne verfügbaren Gruppen zu durchsuchen.
7. Wählen Sie die Gruppe in der Liste **Gruppen-oder Benutzernamen** aus, und aktivieren Sie dann das Kontrollkästchen in der Spalte **verweigern** für die **Gruppenrichtlinie Lesen** und anwenden.
8. Klicken Sie auf **OK**, und klicken Sie dann im Dialogfeld **Windows-Sicherheit** auf **Ja**.
9. Die Gruppe wird in der Liste mit **benutzerdefinierten** Berechtigungen angezeigt.

Ändern des Regelmodus von Anforderung in Voraussetzung

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie bestätigt haben, dass der Netzwerkdatenverkehr mithilfe von IPSec ordnungsgemäß geschützt wird, können Sie die Regeln für die Domänen Isolations-und Verschlüsselungs Zonen so ändern, dass anstelle der Authentifizierung die Authentifizierung erforderlich ist. Ändern Sie die Regeln für die Grenz Zone nicht; Sie müssen im Anforderungsmodus bleiben, damit Geräte in der Grenz Zone weiterhin Verbindungen von Geräten akzeptieren können, die nicht Teil der isolierten Domäne sind.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

In diesem Thema:

So konvertieren Sie eine Regel aus der Anforderung in den require-Modus

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im rechten Navigationsbereich auf **Verbindungssicherheitsregeln**.
3. Doppelklicken Sie im Detailbereich auf die Verbindungssicherheitsregel, die Sie ändern möchten.
4. Klicken Sie auf die Registerkarte **Authentifizierung** .
5. Ändern Sie im Abschnitt **Anforderungen** den **Authentifizierungsmodus** so, dass Sie **eingehende und ausgehende**Nachrichten anfordern, und klicken Sie dann auf **OK**.

So wenden Sie die geänderten GPOs auf die Clientgeräte an

1. Wenn jedes Gerät das nächste Mal seine Gruppenrichtlinie aktualisiert, erhält es das aktualisierte GPO und wendet die geänderte Regel an. Führen Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten aus, um eine sofortige Aktualisierung zu erzwingen:

   ```
   gpupdate /force
   ```

2. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das geänderte GPO ordnungsgemäß auf die Clientgeräte angewendet wurde:

```
gpresult /r /scope computer
```

3. Überprüfen Sie die Befehlsausgabe für die Liste der GPOs, die auf das Gerät angewendet werden, und stellen Sie sicher, dass die Liste die GPOs enthält, die auf dem Gerät angezeigt werden sollen.

Konfigurieren von Authentifizierungsmethoden

10.06.2019 • 4 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Dieses Verfahren zeigt, wie Sie die Authentifizierungsmethoden konfigurieren, die von Computern in einer isolierten Domäne oder einer eigenständigen isolierten Serverzone verwendet werden können.

> **Hinweis:** Wenn Sie die Schritte im Verfahren in diesem Thema ausführen, ändern Sie die systemweiten Standardeinstellungen. Alle Verbindungssicherheitsregeln können diese Einstellungen verwenden, indem Sie auf der Registerkarte **Authentifizierung** die **Standardeinstellung** angeben.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So konfigurieren Sie Authentifizierungsmethoden

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Detailbereich auf der Hauptseite Windows Defender-Firewall mit erweiterter Sicherheit auf **Windows Defender-Firewall-Eigenschaften**.
3. Klicken Sie auf der Registerkarte **IPSec-Einstellungen** auf **Anpassen**.
4. Wählen Sie im Abschnitt **Authentifizierungsmethode** die Art der Authentifizierung aus, die Sie unter den folgenden verwenden möchten:
    a. **Standard**. Wenn Sie diese Option auswählen, wird der Computer angewiesen, die Authentifizierungsmethode zu verwenden, die derzeit vom lokalen Administrator in der Windows Defender-Firewall oder nach Gruppenrichtlinien als Standard definiert ist.
    b. **Computer und Benutzer (mit Kerberos V5)**. Wenn Sie diese Option auswählen, wird der Computer aufgefordert, die Authentifizierung sowohl des Computers als auch des aktuell angemeldeten Benutzers unter Verwendung ihrer Domänenanmeldeinformationen zu verwenden.
    c. **Computer (mit Kerberos V5)**. Wenn Sie diese Option auswählen, wird der Computer über die Domänenanmeldeinformationen zur Verwendung und Authentifizierung des Computers aufgefordert. Diese Option funktioniert mit anderen Computern, die IKE v1 verwenden können, einschließlich früherer Versionen von Windows.
    d. **Benutzer (mit Kerberos V5)**. Wenn Sie diese Option auswählen, wird der Computer angewiesen, die Authentifizierung des aktuell angemeldeten Benutzers mithilfe seiner Domänenanmeldeinformationen zu verwenden und zu erfordern.
    e. **Computer Zertifikat dieser Zertifizierungsstelle** Wenn Sie diese Option auswählen und die Kennung einer Zertifizierungsstelle eingeben, wird der Computer dazu aufgefordert, mithilfe eines Zertifikats, das von der ausgewählten Zertifizierungsstelle ausgestellt wurde, eine Authentifizierung zu verwenden und zu erfordern. Wenn Sie auch **nur Integritätszertifikate akzeptieren**auswählen,

können für diese Regel nur Zertifikate verwendet werden, die in der Regel in einer NAP-Infrastruktur (Network Access Protection, erweiterte Schlüsselverwendung) enthalten sind.

f. **Erweitert**. Klicken Sie auf **Anpassen** , um eine benutzerdefinierte Kombination von Authentifizierungsmethoden anzugeben, die für Ihr Szenario erforderlich sind. Sie können sowohl eine **Erste Authentifizierungsmethode** als auch eine **zweite Authentifizierungsmethode**angeben.

   Die erste Authentifizierungsmethode kann eine der folgenden Methoden sein:

   - **Computer (Kerberos V5)**. Wenn Sie diese Option auswählen, wird der Computer über die Domänenanmeldeinformationen zur Verwendung und Authentifizierung des Computers aufgefordert. Diese Option funktioniert mit anderen Computern, die IKE v1 verwenden können, einschließlich früherer Versionen von Windows.
   - **Computer (NTLMv2)**. Wenn Sie diese Option auswählen, wird der Computer über die Domänenanmeldeinformationen zur Verwendung und Authentifizierung des Computers aufgefordert. Diese Option funktioniert nur mit anderen Computern, die AuthIP verwenden können. Die benutzerbasierte Authentifizierung mit Kerberos V5 wird von IKE v1 nicht unterstützt.
   - **Computer Zertifikat dieser Zertifizierungsstelle (Certification Authority, ca)**. Wenn Sie diese Option auswählen und die ID einer Zertifizierungsstelle eingeben, wird der Computer aufgefordert, mithilfe eines Zertifikats, das von dieser Zertifizierungsstelle ausgestellt wird, eine Authentifizierung zu verwenden. Wenn Sie auch **nur Integritätszertifikate akzeptieren**auswählen, können nur von einem NAP-Server ausgestellte Zertifikate verwendet werden.
   - **Vorgegebener Schlüssel (wird nicht empfohlen)**. Wenn Sie diese Methode auswählen und einen vorinstallierten Schlüssel eingeben, wird der Computer von der Authentifizierung durch Austauschen der vorinstallierten Schlüssel informiert. Wenn Sie übereinstimmen, ist die Authentifizierung erfolgreich. Diese Methode wird nicht empfohlen und ist nur aus Gründen der Abwärtskompatibilität und Tests enthalten.

   Wenn Sie die Option **erste Authentifizierung auswählen ist optional**, kann die Verbindung auch dann erfolgreich sein, wenn der in dieser Spalte angegebene Authentifizierungsversuch fehlschlägt.

   Die zweite Authentifizierungsmethode kann eine der folgenden Methoden sein:

   - **Benutzer (Kerberos V5)**. Wenn Sie diese Option auswählen, wird der Computer angewiesen, die Authentifizierung des aktuell angemeldeten Benutzers mithilfe seiner Domänenanmeldeinformationen zu verwenden und zu erfordern. Diese Authentifizierungsmethode funktioniert nur mit anderen Computern, die AuthIP verwenden können. Die benutzerbasierte Authentifizierung mit Kerberos V5 wird von IKE v1 nicht unterstützt.
   - **Benutzer (NTLMv2)**. Wenn Sie diese Option auswählen, wird der Computer angewiesen, die Authentifizierung des aktuell angemeldeten Benutzers mithilfe seiner Domänenanmeldeinformationen zu verwenden und das NTLMv2-Protokoll anstelle von Kerberos V5 zu verwenden. Diese Authentifizierungsmethode funktioniert nur mit anderen Computern, die AuthIP verwenden können. Die benutzerbasierte Authentifizierung mit Kerberos V5 wird von IKE v1 nicht unterstützt.
   - **Benutzer Integritätszertifikat dieser Zertifizierungsstelle (Certification Authority, ca)**. Wenn Sie diese Option auswählen und die ID einer Zertifizierungsstelle eingeben, wird der Computer aufgefordert, die benutzerbasierte Authentifizierung mithilfe eines Zertifikats zu verwenden, das von der angegebenen Zertifizierungsstelle ausgestellt wurde. Wenn Sie

auch **Zertifikat zur Kontozuordnung aktivieren**auswählen, kann das Zertifikat einem Benutzer in Active Directory zugeordnet werden, um den Zugriff auf bestimmte Benutzer oder Benutzergruppen zu gewähren oder zu verweigern.

- **Computer Integritätszertifikat dieser Zertifizierungsstelle (Certification Authority, ca)**. Wenn Sie diese Option auswählen und die ID einer Zertifizierungsstelle eingeben, wird der Computer aufgefordert, mithilfe eines Zertifikats, das von der angegebenen Zertifizierungsstelle ausgestellt wurde, eine Authentifizierung zu verwenden. Wenn Sie auch **nur Integritätszertifikate akzeptieren**auswählen, können für diese Regel nur Zertifikate verwendet werden, die die EKU "Systemintegritätsauthentifizierung" enthalten, die in der Regel in einer NAP-Infrastruktur bereitgestellt wird.

Wenn Sie die Option **zweite Authentifizierung auswählen ist optional**, kann die Verbindung auch dann erfolgreich sein, wenn der in dieser Spalte angegebene Authentifizierungsversuch fehlschlägt.

> **Wichtig:** Stellen Sie sicher, dass Sie die Kontrollkästchen nicht aktivieren, damit sowohl die erste als auch die zweite Authentifizierung optional ist. Dadurch können nur-Text-Verbindungen verwendet werden, wenn die Authentifizierung fehlschlägt.

5. Klicken Sie in jedem Dialogfeld auf **OK** , um Ihre Änderungen zu speichern und zum Gruppenrichtlinien-Verwaltungs-Editor zurückzukehren.

Konfigurieren von Einstellungen für den Datenschutz (Schnellmodus)

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Verfahren wird gezeigt, wie Sie die Einstellungen für den Datenschutz (Schnellmodus) für Verbindungssicherheitsregeln in einer isolierten Domäne oder einer eigenständigen isolierten Serverzone konfigurieren.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So konfigurieren Sie die Einstellungen für den Schnellmodus

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Detailbereich auf der Hauptseite Windows Defender-Firewall mit erweiterter Sicherheit auf **Windows Defender-Firewall-Eigenschaften**.
3. Klicken Sie auf der Registerkarte **IPSec-Einstellungen** auf **Anpassen**.
4. Klicken Sie im Abschnitt **Datenschutz (Schnellmodus)** auf **erweitert**und dann auf **Anpassen**.
5. Wenn Sie für den gesamten Netzwerkdatenverkehr in der angegebenen Zone eine Verschlüsselung benötigen, aktivieren Sie **für alle Verbindungssicherheitsregeln, die diese Einstellungen verwenden, Verschlüsselung anfordern**. Wenn Sie diese Option auswählen, wird der Abschnitt **Datenintegrität** deaktiviert, und es wird erzwungen, dass Sie nur Integritätsalgorithmen auswählen, die mit einem Verschlüsselungsalgorithmus kombiniert werden. Wenn Sie diese Option nicht auswählen, können Sie nur Daten Integritätsalgorithmen verwenden. Bevor Sie diese Option auswählen, sollten Sie die Auswirkungen auf die Leistung und den dadurch resultierenden Anstieg des Netzwerkverkehrs in Frage stellen. Wir empfehlen, diese Einstellung nur für den Netzwerkdatenverkehr zu verwenden, der Sie wirklich erfordert, beispielsweise zu und von Computern in der Verschlüsselungszone.
6. Wenn Sie keine **Verschlüsselung anfordern**ausgewählt haben, wählen Sie die Daten Integritätsalgorithmen aus, die Sie zum Schutz der Daten Sitzungen zwischen den beiden Computern verwenden möchten. Wenn die in der Liste angezeigten Daten Integritätsalgorithmen nicht Ihre Wünsche sind, gehen Sie folgendermaßen vor:
   a. Entfernen Sie in der linken Spalte alle Daten Integritätsalgorithmen, die Sie nicht benötigen, indem Sie den Algorithmus auswählen und dann auf **Entfernen**klicken.
   b. Fügen Sie alle erforderlichen Daten Integritätsalgorithmen hinzu, indem **Sie auf Hinzufügen**klicken, das entsprechende Protokoll (ESP oder AH) und den Algorithmus (SHA1 oder MD5) auswählen, die Schlüssellebensdauer in Minuten oder Sitzungen auswählen und dann auf **OK**klicken. Wir empfehlen, MD5 nicht in eine beliebige Kombination einzubeziehen. Sie ist nur aus Gründen der Abwärtskompatibilität enthalten. Wir empfehlen außerdem, dass Sie ESP anstelle von

AH verwenden, wenn Sie über Geräte in Ihrem Netzwerk verfügen, die Netzwerkadressübersetzung (Network Address Translation, NAT) verwenden.

c. Geben Sie unter **Schlüssellebensdauer (in Sitzungen)** die Häufigkeit ein, mit der die Schnellmodus-Sitzung erneut eingegeben werden kann. Nachdem diese Zahl erreicht ist, muss die Schnellmodus-Sicherheitszuordnung neu verhandelt werden. Achten Sie darauf, dass Sie die Leistung mit Sicherheitsanforderungen abwägen. Obwohl eine kürzere Schlüssellebensdauer zu einer besseren Sicherheit führt, verringert sich auch die Leistung aufgrund der häufigeren Neuverhandlung der Schnellmodus-Sicherheitszuordnung. Wir empfehlen, den Standardwert zu verwenden, es sei denn, die Risikoanalyse zeigt an, dass ein anderer Wert erforderlich ist.

d. Klicken Sie auf **OK** , um die Kombinations Einstellungen für Algorithmen zu speichern.

e. Nachdem die Liste nur die gewünschten Kombinationen enthält, verwenden Sie die aufwärts-und Abwärtspfeile rechts neben der Liste, um Sie in der richtigen Reihenfolge für den Entwurf neu anzuordnen. Die Algorithmus-Kombination, die zuerst in der Liste enthalten ist, wird zuerst ausprobiert usw.

7. Wählen Sie die Daten Integritäts-und Verschlüsselungsalgorithmen aus, mit denen Sie die Daten Sitzungen zwischen den beiden Computern schützen möchten. Wenn die in der Liste angezeigten Algorithmus Kombinationen nicht Ihren Vorstellungen entsprechend sind, gehen Sie folgendermaßen vor:

   a. Entfernen Sie in der zweiten Spalte alle Daten Integritäts-und Verschlüsselungsalgorithmen, die Sie nicht benötigen, indem Sie die Algorithmus-Kombination auswählen und dann auf **Entfernen**klicken.

   b. Fügen Sie alle erforderlichen Integritäts-und Verschlüsselungsalgorithmus Kombinationen hinzu, indem **Sie auf Hinzufügen**klicken, und gehen Sie dann wie folgt vor:

   c. Wählen Sie das entsprechende Protokoll (ESP oder AH) aus. Wir empfehlen, dass Sie ESP anstelle von AH verwenden, wenn Sie über Geräte in Ihrem Netzwerk verfügen, die NAT verwenden.

   d. Wählen Sie den entsprechenden Verschlüsselungsalgorithmus aus. Die Auswahlmöglichkeiten umfassen in der Reihenfolge der abnehmenden Sicherheit: AES-256, AES-192, AES-128, 3DES und des. Wir empfehlen, dass Sie des nicht in eine beliebige Kombination aufnehmen. Sie ist nur aus Gründen der Abwärtskompatibilität enthalten.

   e. Wählen Sie den entsprechenden Integritätsalgorithmus (SHA1 oder MD5) aus. Wir empfehlen, MD5 nicht in eine beliebige Kombination einzubeziehen. Sie ist nur aus Gründen der Abwärtskompatibilität enthalten.

   f. Geben Sie in die **Schlüssellebensdauer (in Minuten)** die Anzahl der Minuten ein. Wenn die angegebene Anzahl von Minuten abgelaufen ist, ist für alle IPSec-Vorgänge zwischen den beiden Computern, die diesen Schlüssel ausgehandelt haben, ein neuer Schlüssel erforderlich. Achten Sie darauf, dass Sie die Leistung mit Sicherheitsanforderungen abwägen. Obwohl eine kürzere Schlüssellebensdauer zu einer besseren Sicherheit führt, verringert Sie auch die Leistung aufgrund der häufigeren erneuten Eingabe. Wir empfehlen, den Standardwert zu verwenden, es sei denn, die Risikoanalyse zeigt an, dass ein anderer Wert erforderlich ist.

8. Klicken Sie dreimal auf **OK** , um Ihre Einstellungen zu speichern.

Konfigurieren der Gruppenrichtlinie für die automatische Registrierung und für die Bereitstellung von Zertifikaten

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Mithilfe dieses Verfahrens können Sie Gruppenrichtlinien so konfigurieren, dass Clientcomputerzertifikate automatisch registriert und auf den Arbeitsstationen in Ihrem Netzwerk bereitgestellt werden. Führen Sie dieses Verfahren für jedes GPO aus, das IPsec-Verbindungssicherheitsregeln enthält, für die dieses Zertifikat erforderlich ist.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren in der Stammdomäne Ihrer Gesamtstruktur und ein Mitglied der Gruppe Organisations-Admins sein.

So konfigurieren Sie die Gruppenrichtlinie zum automatischen Registrieren von Zertifikaten

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:** *YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, erweitern Sie **Gruppenrichtlinienobjekte**, klicken Sie mit der rechten Maustaste auf das zu ändernde GPO, und klicken Sie dann auf **Bearbeiten**.
3. Erweitern Sie im Navigationsbereich den folgenden Pfad: **Computer Konfiguration**, **Richtlinien**, **Windows-Einstellungen**, **Sicherheitseinstellungen**, **Richtlinien für öffentliche Schlüssel**.
4. Doppelklicken Sie auf **Certificate Services-Client – automatische Registrierung**.
5. Ändern Sie im Dialogfeld **Eigenschaften** das **Konfigurationsmodell** in **aktiviert**.
6. Wählen Sie sowohl **Abgelaufene Zertifikate verlängern, ausstehende Zertifikate aktualisieren und gesperrte Zertifikate entfernen** und **Zertifikate aktualisieren, die Zertifikatvorlagen verwenden**aus.
7. Klicken Sie auf **OK** , um die Änderungen zu speichern. Computer wenden das Gruppenrichtlinienobjekt an und laden das Zertifikat bei der nächsten Aktualisierung der Gruppenrichtlinie herunter.

Konfigurieren von Einstellungen für den Schlüsselaustausch (Hauptmodus)

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Verfahren wird gezeigt, wie Sie die Hauptmodus-Schlüsselaustauscheinstellungen konfigurieren, die zum Sichern des IPSec-Authentifizierungs Verkehrs verwendet werden.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So konfigurieren Sie die Einstellungen für den Schlüsselaustausch

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Detailbereich auf der Hauptseite Windows Defender-Firewall mit erweiterter Sicherheit auf **Windows Defender-Firewall-Eigenschaften**.
3. Klicken Sie auf der Registerkarte **IPSec-Einstellungen** auf **Anpassen**.
4. Klicken Sie im Abschnitt **Schlüsselaustausch (Hauptmodus)** auf **erweitert**und dann auf **Anpassen**.
5. Wählen Sie die Sicherheitsmethoden aus, mit denen Sie die Hauptmodus-Verhandlungen zwischen den beiden Geräten schützen können. Wenn die in der Liste angezeigten Sicherheitsmethoden nicht Ihre Wünsche sind, gehen Sie folgendermaßen vor:

   Wichtig in Windows Vista, Windows Server2008 oder höher können Sie nur einen Schlüsselaustauschalgorithmus angeben. Wenn Sie also mithilfe von IPSec mit einem anderen Gerät unter Windows 8 oder Windows Server 2012 kommunizieren möchten, müssen Sie auf beiden Geräten denselben Schlüsselaustauschalgorithmus auswählen.

   Wenn Sie eine Verbindungssicherheitsregel erstellen, die eine Option angibt, für die AuthIP anstelle von IKE erforderlich ist, wird in der Aushandlung nur die eine Kombination aus der obersten Integritäts-und Verschlüsselungs Sicherheitsmethode verwendet. Stellen Sie sicher, dass alle Ihre Geräte, auf denen mindestens Windows Vista und Windows Server2008 ausgeführt werden, die gleichen Methoden oben in der Liste aufweisen und derselbe Schlüsselaustauschalgorithmus ausgewählt ist.

   Hinweis Wenn AuthIP verwendet wird, wird kein Diffie-Hellman-Schlüsselaustauschprotokoll verwendet. Wenn die KerberosV5-Authentifizierung angefordert wird, wird stattdessen der KerberosV5-Dienstticket Secret anstelle eines Diffie-Hellman-Werts verwendet. Wenn entweder die Zertifikatauthentifizierung oder die NTLM-Authentifizierung angefordert wird, wird eine TLS-Sitzung (Transport Level Security) eingerichtet, und Ihr Kennwort wird anstelle des Diffie-Hellman-Werts verwendet. Dies geschieht unabhängig von dem von Ihnen ausgewählten Diffie-Hellman-Schlüsselaustauschprotokoll.

   a. Entfernen Sie alle gewünschten Sicherheitsmethoden, indem Sie die Methode auswählen und dann auf **Entfernen**klicken.

b. Fügen Sie alle erforderlichen Kombinationen von Sicherheitsmethoden hinzu, indem **Sie auf Hinzufügen**klicken, den entsprechenden Verschlüsselungsalgorithmus und Integritätsalgorithmus aus den Listen auswählen und dann auf **OK**klicken.

> **Vorsicht:** es wird empfohlen, dass Sie keine MD5-oder des-in-Kombinationen angeben. Sie sind nur aus Gründen der Abwärtskompatibilität enthalten.

c. Nachdem die Liste nur die gewünschten Kombinationen enthält, verwenden Sie die aufwärts-und Abwärtspfeile rechts neben der Liste, um Sie in der Reihenfolge der Einstellungen anzuordnen. Die Kombination, die zuerst in der Liste angezeigt wird, wird zuerst ausprobiert usw.

6. Wählen Sie in der Liste auf der rechten Seite den Schlüsselaustauschalgorithmus aus, den Sie verwenden möchten.

> **Vorsicht:** es wird empfohlen, die Diffie-Hellman-Gruppe 1 nicht zu verwenden. Sie ist nur aus Gründen der Abwärtskompatibilität enthalten.

7. Geben Sie in die **Schlüssellebensdauer (in Minuten)** die Anzahl der Minuten ein. Wenn die angegebene Anzahl von Minuten abgelaufen ist, erfordert jeder IPSec-Vorgang zwischen den beiden Geräten einen neuen Schlüssel.

> **Hinweis:** Sie müssen die Leistung mit Sicherheitsanforderungen abwägen. Obwohl eine kürzere Schlüssellebensdauer zu einer besseren Sicherheit führt, verringert sich auch die Leistung.

8. Geben Sie unter **Schlüssellebensdauer (in Sitzungen)** die Anzahl der Sitzungen ein. Nachdem die angegebene Anzahl von Schnellmodus-Sitzungen innerhalb der durch diesen Schlüssel geschützten Sicherheitszuordnung erstellt wurde, erfordert IPSec einen neuen Schlüssel.
9. Klicken Sie dreimal auf **OK** , um Ihre Einstellungen zu speichern.

Konfigurieren der Regeln für eine zwingend erforderliche Verschlüsselung

07.06.2019 • 2 minutes to read

Wenn Sie eine Zone erstellen, für die eine Verschlüsselung erforderlich ist, müssen Sie die Regeln so konfigurieren, dass die Verschlüsselungsalgorithmen hinzugefügt und die Algorithmus Kombinationen, die keine Verschlüsselung verwenden, gelöscht werden.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über die Berechtigung zum Ändern der GPOs verfügen.

So ändern Sie eine Authentifizierungs Anforderungs Regel, um auch eine Verschlüsselung zu erfordern

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Verbindungssicherheitsregeln**.
3. Doppelklicken Sie im Detailbereich auf die Verbindungssicherheitsregel, die Sie ändern möchten.
4. Benennen Sie auf der Seite **Name** die Verbindungssicherheitsregel um, bearbeiten Sie die Beschreibung so, dass Sie die neue Verwendung für die Regel widerspiegelt, und klicken Sie dann auf **OK**.
5. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Windows Defender Firewall – LDAP://CN = {*GUID*}**, und klicken Sie dann auf **Eigenschaften**.
6. Klicken Sie auf die Registerkarte **IPSec-Einstellungen** .
7. Klicken Sie unter **IPsec-Standardeinstellungen**auf **Anpassen**.
8. Klicken Sie unter **Datenschutz (Schnellmodus)** auf **erweitert**und dann auf **Anpassen**.
9. Klicken Sie auf **Verschlüsselung für alle Verbindungssicherheitsregeln anfordern, die diese Einstellungen verwenden**.

   Dadurch wird der Abschnitt Daten Integritätsregeln deaktiviert. Stellen Sie sicher, dass die Liste **Datenintegrität und Verschlüsselung** alle Kombinationen enthält, die von ihren Clientgeräten für die Verbindung mit Mitgliedern des Verschlüsselungs Bereichs verwendet werden. Die Clientgeräte erhalten ihre Regeln über das Gruppenrichtlinienobjekt für die Zone, in der Sie sich befinden. Sie müssen sicherstellen, dass diese Regeln mindestens einen der Daten Integritäts-und Verschlüsselungsalgorithmen enthalten, die in dieser Regel konfiguriert sind, oder die Clientgeräte in dieser Zone können keine Verbindung zu Geräten in dieser Zone herstellen.
10. Wenn Sie eine Kombination aus Algorithmen hinzufügen müssen, klicken Sie auf **Hinzufügen**, und wählen Sie dann die Kombination aus Verschlüsselungs-und Integritätsalgorithmen aus. Die Optionen sind unter Konfigurieren von Datenschutzeinstellungen (Schnellmodus)beschrieben.

    Hinweis nicht alle in Windows 8 oder Windows Server 2012 und höher verfügbaren Algorithmen können in der Windows Defender-Firewall mit erweiterter Sicherheit auf der Benutzeroberfläche ausgewählt werden. Sie können Windows PowerShell verwenden, um Sie auszuwählen.

    Die Einstellungen für den Schnellmodus können auch regelmäßig konfiguriert werden, jedoch nicht über die Benutzeroberfläche der Windows Defender-Firewall. Stattdessen können Sie die Regeln mithilfe von

Windows PowerShell erstellen oder ändern.

Weitere Informationen finden Sie unter Windows Defender-Firewall mit erweiterter Sicherheitsverwaltung mit Windows PowerShell .

11. Während der Aushandlung werden Algorithmus Kombinationen in der Reihenfolge vorgeschlagen, die in der Liste angezeigt wird. Stellen Sie sicher, dass die sichereren Kombinationen oben in der Liste stehen, damit die Verhandlungs Geräte die sicherste Kombination auswählen, die Sie gemeinsam unterstützen können.

12. Klicken Sie dreimal auf **OK** , um die Änderungen zu speichern.

Konfigurieren der Windows Defender-Firewall mit erweitertem Sicherheitsprotokoll

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Wenn Sie die Windows Defender-Firewall mit erweiterter Sicherheit konfigurieren möchten, um verworfene Pakete oder erfolgreiche Verbindungen zu protokollieren, verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit im MMC-Snap-in Gruppenrichtlinienverwaltung.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So konfigurieren Sie die Windows Defender-Firewall mit erweitertem Sicherheitsprotokoll

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Detailbereich im Abschnitt **Übersicht** auf Eigenschaften von **Windows Defender-Firewall**.
3. Führen Sie für jeden Netzwerkadresstyp (Domäne, privat, öffentlich) die folgenden Schritte aus.
   a. Klicken Sie auf die Registerkarte, die dem Typ des Netzwerkspeicherorts entspricht.
   b. Klicken Sie unter **Protokollierung**auf **Anpassen**.
   c. Der Standardpfad für das Protokoll lautet **%windir%\system32\logfiles\firewall\pfirewall.log**. Wenn Sie dies ändern möchten, deaktivieren Sie das Kontrollkästchen **nicht konfiguriert** , geben Sie den Pfad zum neuen Speicherort ein, oder klicken Sie auf **Durchsuchen** , um einen Dateispeicherort auszuwählen.

      > **Wichtig:** der angegebene Speicherort muss über Berechtigungen verfügen, die dem Windows Defender-Firewalldienst das Schreiben in die Protokolldatei gestatten.

   d. Die standardmäßige maximale Dateigröße für das Protokoll ist 4.096 Kilobyte (KB). Wenn Sie dies ändern möchten, deaktivieren Sie das Kontrollkästchen **nicht konfiguriert** , und geben Sie die neue Größe in KB ein, oder verwenden Sie die nach-oben-und nach-unten-Taste, um eine Größe auszuwählen. Die Datei wird nicht über diese Größe hinaus vergrößert. Wenn das Limit erreicht ist, werden alte Protokolleinträge gelöscht, um Platz für die neu erstellten zu schaffen.
   e. Es erfolgt keine Protokollierung, bis Sie eine der folgenden beiden Optionen eingerichtet haben:
      - Wenn Sie einen Protokolleintrag erstellen möchten, wenn die Windows Defender-Firewall ein eingehendes Netzwerkpaket abbricht, ändern Sie **verworfene Pakete** auf **Ja**.
      - Wenn Sie einen Protokolleintrag erstellen möchten, wenn die Windows Defender-Firewall eine eingehende Verbindung zulässt, ändern Sie **erfolgreiche Verbindungen**

protokollieren in **Ja**.

f. Klicken Sie zweimal auf **OK** .

Problembehandlung bei der Aufnahme langsamer Protokolle

Wenn Protokolle in Sentinel langsam angezeigt werden, können Sie die Größe der Protokolldatei verringern. Beachten Sie, dass dies aufgrund der erhöhten Ressourcennutzung für die Protokollrotation zu mehr Ressourcennutzung führt.

Konfigurieren der Zertifikatvorlage zur Arbeitsstationsauthentifizierung

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

In diesem Verfahren wird beschrieben, wie Sie eine Zertifikatvorlage konfigurieren, die von der Active Directory-Zertifizierungsdienste (MDE) als Ausgangspunkt für Gerätezertifikate verwendet wird, die automatisch registriert und auf Workstations in der Domäne bereitgestellt werden. Es wird gezeigt, wie Sie eine Kopie einer Vorlage erstellen und dann die Vorlage entsprechend ihren Entwurfsanforderungen konfigurieren.

Administrative Anmeldeinformationen

So konfigurieren Sie die Zertifikatvorlage für Workstation-Authentifizierung und die automatische Registrierung

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren in der Stammdomäne Ihrer Gesamtstruktur und ein Mitglied der Gruppe Organisations-Admins sein.

1. Öffnen Sie auf dem Gerät, auf dem MDE installiert ist, die Konsole Zertifizierungsstelle.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Zertifikatvorlagen**, und klicken Sie dann auf **Verwalten**.
3. Klicken Sie im Detailbereich auf die Vorlage **Workstation-Authentifizierung** .
4. Klicken Sie im Menü **Aktion** auf **Vorlage duplizieren**. Wählen Sie im Dialogfeld **Vorlage duplizieren** die Vorlagenversion aus, die für die Bereitstellung geeignet ist, und klicken Sie dann auf **OK**. Damit die resultierenden Zertifikate maximale Kompatibilität mit den verfügbaren Versionen von Windows aufweisen, sollten Sie **WindowsServer2003**auswählen.
5. Geben Sie auf der Registerkarte **Allgemein** unter **Vorlagenanzeigename**einen neuen Namen für die Zertifikatvorlage ein, beispielsweise eine **Authentifizierungs Vorlage für die Domänen Isolierungs Arbeitsstation**.
6. Klicken Sie auf die Registerkarte **Antragsteller Name** . Stellen Sie sicher, dass **Build aus diesen Active Directory-Informationen** ausgewählt ist. Wählen Sie im **Format Antragstellername**den Eintrag **Vollständiger Name**aus.
7. Klicken Sie auf die Registerkarte **Kryptografie** . Sie müssen die optimale minimale Schlüsselgröße für Ihre Umgebung ermitteln. Große Schlüsselgrößen bieten eine bessere Sicherheit, können sich aber auf die Serverleistung auswirken. Wir empfehlen, dass Sie die Standardeinstellung 2048 verwenden.
8. Klicken Sie auf die Registerkarte **Sicherheit** . Klicken Sie in **Gruppen-oder Benutzernamen**auf **Domänencomputer**, wählen Sie unter **zulassen**die Option **registrieren** und automatisch **registrieren**aus, und klicken Sie dann auf **OK**.

> **Hinweis:** Wenn Sie das Zertifikat nicht auf allen Geräten in der Domäne bereitstellen möchten, geben Sie eine andere Gruppe oder Gruppen an, die die Geräte Konten enthalten, die das Zertifikat empfangen

> sollen.

9. Schließen Sie die Konsole Zertifikatvorlagen.
10. Klicken Sie im MMC-Snap-In Zertifizierungsstelle im linken Bereich mit der rechten Maustaste auf **Zertifikatvorlagen**, klicken Sie auf **neu**, und klicken Sie dann auf **Zertifikatvorlage zum ausgeben**.
11. Klicken Sie im Dialogfeld **Zertifikatvorlagen aktivieren** auf den Namen der soeben konfigurierten Zertifikatvorlage, und klicken Sie dann auf **OK**.

Konfigurieren der Windows Defender-Firewall mit erweiterter Sicherheit, um Benachrichtigungen zu unterdrücken, wenn ein Programm blockiert wird

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

So konfigurieren Sie die Windows Defender-Firewall mit erweiterter Sicherheit, um die Anzeige einer Benachrichtigung zu unterdrücken, wenn Sie ein Programm blockiert, das versucht, auf Netzwerkdatenverkehr zu lauschen und lokal definierte Regeln zu untersagen, verwenden Sie die Windows Defender-Firewall mit erweiterter Sicherheit. Knoten in der Gruppenrichtlinien-Verwaltungskonsole.

> **Achtung:** Wenn Sie Benachrichtigungen deaktivieren und lokal definierte Regeln untersagen möchten, müssen Sie Firewallregeln erstellen, mit denen die Programme Ihrer Benutzer den erforderlichen Netzwerkdatenverkehr senden und empfangen können. Wenn keine Firewall-Regel vorhanden ist, erhält der Benutzer keine Art von Warnung, der Netzwerkdatenverkehr wird automatisch blockiert, und das Programm schlägt möglicherweise fehl.

Es wird empfohlen, diese Einstellungen erst zu aktivieren, nachdem Sie die erforderlichen Regeln erstellt und getestet haben.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So konfigurieren Sie die Windows Defender-Firewall so, dass die Anzeige einer Benachrichtigung für ein blockiertes Programm unterdrückt und lokal definierte Regeln ignoriert werden

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Detailbereich im Abschnitt **Übersicht** auf Eigenschaften von **Windows Defender-Firewall**.
3. Führen Sie für jeden Netzwerkadresstyp (Domäne, privat, öffentlich) die folgenden Schritte aus.
    a. Klicken Sie auf die Registerkarte, die dem Typ des Netzwerkspeicherorts entspricht.
    b. Klicken Sie unter **Einstellungen**auf **Anpassen**.
    c. Ändern **** Sie unter Firewalleinstellungen **Anzeige eine Benachrichtigung** auf **Nein**.
    d. Ändern Sie unter **Regelzusammenführung**die **Richtlinien für lokale Firewall** auf **Nein**anwenden.
    e. Obwohl eine Verbindungssicherheitsregel keine Firewall-Einstellung ist, können Sie diese Registerkarte auch verwenden, um lokal definierte Verbindungssicherheitsregeln zu untersagen,

wenn Sie planen, IPSec-Regeln als Teil einer Server-oder Domänenisolierungsumgebung bereitzustellen. Ändern Sie unter **Regelzusammenführung**die **Richtlinien für die lokale Verbindungssicherheit** auf **Nein**.

f. Klicken Sie zweimal auf **OK** .

Bestätigen, dass Zertifikate ordnungsgemäß bereitgestellt werden

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie Ihre Zertifikate und die automatische Registrierung in Gruppenrichtlinien konfiguriert haben, können Sie sicherstellen, dass die Richtlinie wie erwartet angewendet wird und dass die Zertifikate ordnungsgemäß auf den Workstation-Geräten installiert werden.

In diesen Verfahren aktualisieren Sie die Gruppenrichtlinie auf einem Clientgerät und stellen dann sicher, dass das Zertifikat ordnungsgemäß bereitgestellt wird.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

In diesem Thema:

So aktualisieren Sie die Gruppenrichtlinie auf einem Gerät

Führen Sie an einer Eingabeaufforderung mit erhöhten Rechten den folgenden Befehl aus:

```
gpupdate /target:computer /force
```

Nachdem die Gruppenrichtlinie aktualisiert wurde, können Sie sehen, welche GPOs aktuell auf das Gerät angewendet werden.

So überprüfen Sie, ob ein Zertifikat installiert ist

1. Öffnen Sie die Zertifikate-Konsole.
2. Erweitern Sie im Navigationsbereich **Vertrauenswürdige Stammzertifizierungsstellen**, und klicken Sie dann auf **Zertifikate**.

   Die von Ihnen erstellte Zertifizierungsstelle wird in der Liste angezeigt.

Kopieren eines Gruppenrichtlinienobjekts zum Erstellen eines neuen Gruppenrichtlinienobjekts

10.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie das Gruppenrichtlinienobjekt für die Grenzzonen Geräte erstellen möchten, erstellen Sie eine Kopie des Hauptgruppen Richtlinienobjekts für die Domänenisolierung, und ändern Sie dann die Einstellungen auf Request (anstelle von require, Authentifizierung). Verwenden Sie zum Erstellen einer Kopie eines GPO das MMC-Snap-in Active Directory-Benutzer und-Geräte.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über Delegierte Berechtigungen zum Erstellen neuer GPOs verfügen.

So erstellen Sie eine Kopie eines Gruppenrichtlinienobjekts

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:***YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, und klicken Sie dann auf **Gruppenrichtlinienobjekte**.
3. Klicken Sie im Detailbereich mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, das Sie kopieren möchten, und klicken Sie dann auf **Kopieren**.
4. Klicken Sie im Navigationsbereich erneut mit der rechten Maustaste auf **Gruppenrichtlinienobjekte** , und klicken Sie dann auf **Einfügen**.
5. Klicken Sie im Dialogfeld **GPO kopieren** auf **vorhandene Berechtigungen beibehalten**, und klicken Sie dann auf **OK**. Wenn Sie diese Option auswählen, werden alle Ausnahmegruppen beibehalten, für die Sie die Berechtigungen zum Lesen und Anwenden von Gruppenrichtlinienobjekten verweigert haben, wodurch die Änderung vereinfacht wird.
6. Klicken Sie nach Abschluss der Kopie auf **OK**. Das neue GPO hat den Namen **Kopie des** *ursprünglichen GPO-namens*.
7. Wenn Sie ihn umbenennen möchten, klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, und klicken Sie dann auf **Umbenennen**.
8. Geben Sie den neuen Namen ein, und drücken Sie dann die EINGABETASTE.
9. Sie müssen die Sicherheitsfilter ändern, um die Richtlinie auf die richtige Gruppe von Geräten anzuwenden. Klicken Sie dazu auf die Registerkarte **Bereich** , und wählen Sie im Abschnitt **Sicherheitsfilterung** die Gruppe aus, die allen Mitgliedern der isolierten Domäne Berechtigungen gewährt, beispielsweise **CG_DOMISO_IsolatedDomain**, und klicken Sie dann auf **Entfernen**.
10. Klicken Sie im Bestätigungsdialogfeld auf **OK**.
11. Klicken Sie auf **Hinzufügen**.
12. Geben Sie den Namen der Gruppe ein, die Mitglieder der Grenz Zone enthält, beispielsweise

CG_DOMISO_Boundary, und klicken Sie dann auf **OK**.

13. Ändern Sie bei Bedarf den WMI-Filter in einen geeigneten für das neue Gruppenrichtlinienobjekt. Wenn das ursprüngliche GPO beispielsweise für Clientgeräte unter Windows 10 und das neue Gruppenrichtlinienobjekt für Grenzzonen für Geräte mit Windows Server 2016 ist, wählen Sie einen WMI-Filter aus, mit dem nur diese Geräte das Gruppenrichtlinienobjekt lesen und anwenden können.

Erstellen eines Gruppenkontos in Active Directory

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Verwenden Sie die Konsole Active Directory-Benutzer und-Computer, um eine Sicherheitsgruppe zu erstellen, die die Computerkonten für die Computer enthält, die eine Gruppe von Gruppenrichtlinieneinstellungen erhalten sollen.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über Delegierte Berechtigungen zum Erstellen neuer Gruppenkonten verfügen.

So fügen Sie eine neue Mitgliedschaftsgruppe in Active Directory hinzu

1. Öffnen Sie die Konsole "Active Directory-Benutzer und-Computer".
2. Wählen Sie im Navigationsbereich den Container aus, in dem Ihre Gruppe gespeichert werden soll. Dies ist normalerweise der **Benutzer** Container unter der Domäne.
3. Klicken Sie auf **Aktion**, klicken Sie auf **neu**, und klicken Sie dann auf **Gruppieren**.
4. Geben Sie im Textfeld **Gruppenname** den Namen für die neue Gruppe ein.

   > **Hinweis:** verwenden Sie einen Namen, der den Zweck eindeutig angibt. Überprüfen Sie, ob Ihre Organisation über eine Benennungskonvention für Gruppen verfügt.

5. Geben Sie im Textfeld **Beschreibung** eine Beschreibung des Zwecks dieser Gruppe ein.
6. Wählen Sie im Abschnitt **Gruppenbereich** entweder **Global** oder **universell**aus, je nach Ihrer Active Directory-Gesamtstruktur. Wenn Ihre Gruppe Computer aus mehreren Domänen einbeziehen muss, wählen Sie **universell**aus. Wenn alle Mitglieder aus der gleichen Domäne sind, wählen Sie **Global**aus.
7. Klicken Sie **** im Abschnitt Gruppentyp auf **Sicherheit**.
8. Klicken Sie auf **OK** , um Ihre Gruppe zu speichern.

Erstellen eines Gruppenrichtlinienobjekts

10.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Verwenden Sie zum Erstellen eines neuen Gruppenrichtlinienobjekts das MMC-Snap-in Active Directory-Benutzer und-Computer.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über Delegierte Berechtigungen zum Erstellen neuer GPOs verfügen.

So erstellen Sie ein neues Gruppenrichtlinienobjekt

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:***YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, und klicken Sie dann auf **Gruppenrichtlinienobjekte**.
3. Klicken Sie auf **Aktion**und dann auf **neu**.
4. Geben Sie im Textfeld **Name** den Namen für das neue Gruppenrichtlinienobjekt ein.

   > **Hinweis:** Verwenden Sie unbedingt einen Namen, der den Zweck des Gruppenrichtlinienobjekts eindeutig angibt. Überprüfen Sie, ob Ihre Organisation über eine Benennungskonvention für GPOs verfügt.

5. Legen Sie das **Starter-Gruppenrichtlinienobjekt** auf **(keine)**, und klicken Sie dann auf **OK**.
6. Wenn das Gruppenrichtlinienobjekt keine Benutzereinstellungen enthält, können Sie die Leistung verbessern, indem Sie den Abschnitt **Benutzerkonfiguration** des Gruppenrichtlinienobjekts deaktivieren. Führen Sie dazu die folgenden Schritte aus:
   a. Klicken Sie im Navigationsbereich auf das neue Gruppenrichtlinienobjekt.
   b. Klicken Sie im Detailbereich auf die Registerkarte **Details** .
   c. Ändern Sie den **GPO-Status** in **Benutzerkonfigurationseinstellungen deaktiviert**.

Erstellen einer Regel mit Authentifizierungsausnahmenliste

10.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In fast jedem Szenario mit isolierten Servern oder isolierten Domänen gibt es einige Geräte oder Geräte, die mit IPSec nicht kommunizieren können. Dieses Verfahren zeigt, wie Sie Regeln erstellen, die diese Geräte von den Authentifizierungsanforderungen ihrer Isolierungs Richtlinien ausschließen.

Wichtig das Hinzufügen von Geräten zur Ausnahmeliste für eine Zone verringert die Sicherheit, da es Geräten in der Zone ermöglicht, Netzwerkdatenverkehr zu senden, der durch IPSec auf die Geräte in der Liste nicht geschützt ist. Wie im Design Handbuch für Windows Defender-Firewall mit erweiterter Sicherheit erläutert, müssen Sie der Ausnahmeliste nur verwaltete und vertrauenswürdige Geräte hinzufügen.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So erstellen Sie eine Regel, die angegebene Hosts von der Authentifizierung ausgenommen

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Verbindungssicherheitsregeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue Verbindungssicherheitsregel auf **Authentifizierungsausnahme**, und klicken Sie dann auf **weiter**.
5. Klicken Sie auf der Seite **Ausgeschlossene Computer** auf **Hinzufügen**, um eine neue Ausnahme zu erstellen. Wenn Sie eine vorhandene Ausnahme ändern möchten, klicken Sie darauf, und klicken Sie dann auf **Bearbeiten**.
6. Führen Sie im Dialogfeld **IP-Adresse** eine der folgenden Aktionen aus:
   - Wenn Sie eine einzelne IP-Adresse hinzufügen möchten, klicken Sie auf **diese IP-Adresse oder das Subnetz**, geben Sie die IP-Adresse des Hosts in das Textfeld ein, und klicken Sie dann auf **OK**.
   - Wenn Sie ein gesamtes Subnetz nach Adresse hinzufügen möchten, klicken Sie auf **diese IP-Adresse oder ein Subnetz**, und geben Sie dann die IP-Adresse des Subnets, gefolgt von einem Schrägstrich (/) und der Anzahl der Bits in der entsprechenden Subnetzmaske ein. **10.50.0.0/16** stellt beispielsweise das Subnetz der Klasse B dar, das mit der Adresse 10.50.0.1 beginnt und mit der Adresse **10.50.255.254**endet. Klicken Sie abschließend auf **OK** .
   - Wenn Sie das Subnetz des lokalen Geräts hinzufügen möchten, klicken Sie auf vordefinierte **Gruppe von Computern**, wählen Sie **Lokales Subnetz** in der Liste aus, und klicken Sie dann auf **OK**.

> **Hinweis:** Wenn Sie das lokale Subnetz aus der Liste auswählen, anstatt die Subnetz-Adresse manuell einzugeben, passt das Gerät das aktive lokale Subnetz automatisch an die aktuelle IP-Adresse des Geräts an.

- Wenn Sie einen diskreten Adressbereich hinzufügen möchten, der keinem Subnetz entspricht, klicken Sie auf **diesen IP-Adressbereich**, geben Sie die Anfangs-und endip-Adressen in die Textfelder **von** und **bis** ein, und klicken Sie dann auf **OK**.
- Wenn Sie alle Remotehosts, die das lokale Gerät für einen angegebenen Netzwerkdienst verwendet, ausnehmen möchten, klicken Sie auf vordefinierte **Gruppe von Computern**, wählen Sie den Netzwerkdienst in der Liste aus, und klicken Sie dann auf **OK**.

7. Wiederholen Sie die Schritte 5 und 6 für jede Freistellung, die Sie erstellen müssen.
8. Klicken Sie auf **weiter** , wenn Sie alle Ausnahmen erstellt haben.
9. Überprüfen Sie auf der Seite **Profil** das Profil für jeden Netzwerkstandorttyp, für den diese Ausnahmen gelten, und klicken Sie dann auf **weiter**.

   > **Vorsicht:** wenn sich alle Ausnahmen im Netzwerk der Organisation befinden und dieses Netzwerk von einer Active Directory-Domäne verwaltet wird, sollten Sie die Regel nur auf das Domänenprofil einschränken. Wenn Sie das falsche Profil auswählen, kann der Schutz für Ihren Computer verringert werden, da sich jeder Computer mit einer IP-Adresse, die einer Ausnahmeregel entspricht, nicht authentifizieren muss.

10. Geben Sie auf der Seite **Name** den Namen der Ausnahmeregel ein, geben Sie eine Beschreibung ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen einer Authentifizierungsanforderungsregel

01.06.2019 • 5 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie IPsec-Algorithmen und Authentifizierungsmethoden konfiguriert haben, können Sie die Regel erstellen, die erfordert, dass die Geräte im Netzwerk diese Protokolle und Methoden verwenden, bevor Sie kommunizieren können.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über die Berechtigung zum Ändern der GPOs verfügen.

So erstellen Sie die Regel für die Authentifizierungsanforderung

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Verbindungssicherheitsregeln**, und klicken Sie dann auf **neue Regel**.
3. Wählen Sie **** auf der Seite Regeltyp die Option **Isolierung**aus, und klicken Sie dann auf **weiter**.
4. Wählen Sie auf der Seite **Anforderungen** die Option **Authentifizierung für eingehende und ausgehende Verbindungen anfordern**aus.

   > **Vorsicht:** konfigurieren Sie die Regel nicht so, dass die eingehende Authentifizierung erforderlich ist, bis Sie bestätigt haben, dass alle Ihre Geräte die richtigen GPOs empfangen, und Sie erfolgreich IPSec aushandeln und sich gegenseitig authentifizieren. Das zulassen, dass die Geräte auch bei einem Authentifizierungsfehler kommunizieren, verhindert, dass Fehler in den GPOs oder deren Verteilung die Kommunikation in Ihrem Netzwerk unterbrechen.

5. Wählen Sie auf der Seite **Authentifizierungsmethode** die Authentifizierungsoption aus, die Sie in Ihrem Netzwerk verwenden möchten. Klicken Sie auf **erweitert**, klicken Sie auf **Anpassen**, und klicken Sie dann auf **Hinzufügen** , um der Liste Methoden hinzuzufügen, um mehrere Methoden auszuwählen, die in der Reihenfolge versucht werden, bis eine erfolgreich ist. Für die zweite Authentifizierungsmethode ist eine authentifizierte IP (AuthIP) erforderlich.

   a. **Standard**. Wenn Sie diese Option auswählen, wird das Gerät aufgefordert, die Authentifizierung mithilfe der derzeit als Standard auf dem Gerät definierten Methode anzufordern. Dieser Standardwert wurde möglicherweise konfiguriert, wenn das Betriebssystem installiert oder durch eine Gruppenrichtlinie konfiguriert wurde. Die Auswahl dieser Option ist geeignet, wenn Sie systemweite Einstellungen mithilfe des Verfahrens zum Konfigurieren von Authentifizierungsmethoden konfiguriert haben.

   b. **Computer und Benutzer (KerberosV5)**. Wenn Sie diese Option auswählen, wird das Gerät angewiesen, die Authentifizierung sowohl des Geräts als auch des aktuell angemeldeten Benutzers mithilfe seiner Domänenanmeldeinformationen anzufordern. Diese Authentifizierungsmethode funktioniert nur mit anderen Geräten, die AuthIP verwenden können. Die benutzerbasierte

Authentifizierung mithilfe von KerberosV5 wird von ikev1 nicht unterstützt.

c. **Computer (KerberosV5)**. Wenn Sie diese Option auswählen, wird das Gerät aufgefordert, die Authentifizierung des Geräts mithilfe seiner Domänenanmeldeinformationen anzufordern. Diese Option funktioniert mit anderen Geräten, als ikev1 verwenden können, einschließlich früherer Versionen von Windows.

d. **Erweitert**. Klicken Sie auf **Anpassen** , um eine benutzerdefinierte Kombination von Authentifizierungsmethoden anzugeben, die für Ihr Szenario erforderlich sind. Sie können sowohl eine **Erste Authentifizierungsmethode** als auch eine **zweite Authentifizierungsmethode**angeben.

   Die **Erste Authentifizierungsmethode** kann eine der folgenden Methoden sein:

   - **Computer (KerberosV5)**. Wenn Sie diese Option auswählen, wird das Gerät aufgefordert, die Authentifizierung des Geräts mithilfe seiner Domänenanmeldeinformationen anzufordern. Diese Option funktioniert mit anderen Geräten, als ikev1 verwenden können, einschließlich früherer Versionen von Windows.
   - **Computer (NTLMv2)**. Wenn Sie diese Option auswählen, wird das Gerät mithilfe seiner Domänenanmeldeinformationen für die Verwendung und Authentifizierung des Geräts benötigt. Diese Option funktioniert nur mit anderen Geräten, die AuthIP verwenden können. Die benutzerbasierte Authentifizierung mithilfe von KerberosV5 wird von ikev1 nicht unterstützt.
   - **Computer Zertifikat dieser Zertifizierungsstelle (Certification Authority, ca)**. Wenn Sie diese Option auswählen und die Kennung einer Zertifizierungsstelle eingeben, wird das Gerät aufgefordert, die Authentifizierung mithilfe eines Zertifikats anzufordern, das von der angegebenen Zertifizierungsstelle ausgestellt wurde. Wenn Sie auch **nur Integritätszertifikate akzeptieren**auswählen, können nur von einem NAP-Server ausgestellte Zertifikate für diese Regel verwendet werden.
   - **Vorgegebener Schlüssel (wird nicht empfohlen)**. Wenn Sie diese Methode auswählen und einen vorab freigegebenen Schlüssel eingeben, wird das Gerät durch Austauschen der vorinstallierten Schlüssel authentifiziert. Wenn die Schlüssel übereinstimmen, ist die Authentifizierung erfolgreich. Diese Methode wird nicht empfohlen und ist nur aus Gründen der Abwärtskompatibilität und zu Testzwecken enthalten.

   Wenn Sie die Option **erste Authentifizierung auswählen ist optional**, kann die Verbindung auch dann erfolgreich sein, wenn der in dieser Spalte angegebene Authentifizierungsversuch fehlschlägt.

   Die **zweite Authentifizierungsmethode** kann eine der folgenden Methoden sein:

   - **Benutzer (KerberosV5)**. Wenn Sie diese Option auswählen, wird das Gerät dazu aufgefordert, die Authentifizierung des aktuell angemeldeten Benutzers mithilfe seiner Domänenanmeldeinformationen zu verwenden. Diese Authentifizierungsmethode funktioniert nur mit anderen Geräten, die AuthIP verwenden können. Die benutzerbasierte Authentifizierung mithilfe von KerberosV5 wird von ikev1 nicht unterstützt.
   - **Benutzer (NTLMv2)**. Wenn Sie diese Option auswählen, wird das Gerät dazu aufgefordert, die Authentifizierung des aktuell angemeldeten Benutzers mithilfe seiner Domänenanmeldeinformationen zu verwenden, und es wird anstelle von KerberosV5 das NTLMv2-Protokoll verwendet. Diese Authentifizierungsmethode funktioniert nur mit anderen Geräten, die AuthIP verwenden können. Die benutzerbasierte Authentifizierung mit NTLMv2 wird von ikev1 nicht unterstützt.
   - **Benutzer Integritätszertifikat dieser Zertifizierungsstelle (Certification Authority, ca)**.

Wenn Sie diese Option auswählen und die Kennung einer Zertifizierungsstelle eingeben, wird das Gerät aufgefordert, die benutzerbasierte Authentifizierung mithilfe eines Zertifikats anzufordern, das von der angegebenen Zertifizierungsstelle ausgestellt wurde. Wenn Sie auch **Zertifikat zur Kontozuordnung aktivieren**auswählen, kann das Zertifikat einem Benutzer in Active Directory zugeordnet werden, um bestimmten Benutzern oder Benutzergruppen den Zugriff zu gewähren oder zu verweigern.

- **Computer Integritätszertifikat dieser Zertifizierungsstelle (Certification Authority, ca)**. Wenn Sie diese Option auswählen und die Kennung einer Zertifizierungsstelle eingeben, wird das Gerät dazu aufgefordert, mithilfe eines Zertifikats, das von der angegebenen Zertifizierungsstelle ausgestellt wurde, eine Authentifizierung zu verwenden. Wenn Sie auch **nur Integritätszertifikate akzeptieren**auswählen, können nur von einem NAP-Server ausgestellte Zertifikate für diese Regel verwendet werden.

Wenn Sie überprüfen, dass die **zweite Authentifizierung optional ist**, kann die Verbindung erfolgreich sein, auch wenn der in dieser Spalte angegebene Authentifizierungsversuch fehlschlägt.

> **Wichtig:** stellen Sie sicher, dass Sie die Kontrollkästchen nicht aktivieren, damit sowohl die erste als auch die zweite Authentifizierung optional sind. Dadurch können nur-Text-Verbindungen verwendet werden, wenn die Authentifizierung fehlschlägt.

6. Nachdem Sie die Authentifizierungsmethoden konfiguriert haben, klicken Sie in jedem Dialogfeld auf **OK** , um Ihre Änderungen zu speichern und zu schließen, bis Sie im Assistenten zur Seite **Authentifizierungsmethode** zurückkehren. Klicken Sie auf **Weiter**.
7. Aktivieren Sie auf der **Profil** Seite die Kontrollkästchen für die Profile des Netzwerkstandorttyps, für die diese Regel gilt.

   - Auf tragbaren Geräten sollten Sie die **privaten** und **öffentlichen** Felder deaktivieren, damit das Gerät ohne Authentifizierung kommunizieren kann, wenn es sich nicht im Domänennetzwerk befindet.
   - Bei Geräten, die nicht von Netzwerk zu Netzwerk wechseln, sollten Sie alle Profile auswählen. Dadurch wird verhindert, dass ein unerwarteter Switch in der Netzwerk Adressart die Regel deaktiviert.

   Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **Name** einen Namen für die Verbindungssicherheitsregel und eine Beschreibung ein, und klicken Sie dann auf **Fertig stellen**.

   Die neue Regel wird in der Liste der Verbindungssicherheitsregeln angezeigt.

Erstellen einer ICMP-Eingangsregel

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Zum Zulassen des eingehenden ICMP-Netzwerkverkehrs (Internet Control Message Protocol) verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit im MMC-Snap-in Gruppenrichtlinienverwaltung, um Firewallregeln zu erstellen. Mit diesem Regeltyp können ICMP-Anforderungen und-Antworten von Computern im Netzwerk gesendet und empfangen werden.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

In diesem Thema wird beschrieben, wie Sie eine Port Regel erstellen, die eingehenden ICMP-Netzwerkdatenverkehr zulässt. Informationen zu anderen Regeltypen für eingehende Ports finden Sie unter:

- Erstellen einer Porteingangsregel
- Erstellen von Eingangsregeln zur RPC-Unterstützung

So erstellen Sie eine eingehende ICMP-Regel

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Eingehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.
5. Klicken Sie auf der Seite **Programm** auf **Alle Programme**, und klicken Sie dann auf **weiter**.
6. Wählen Sie auf der Seite **Protokoll und Ports** in der Liste Protokolltyp **** die Option **ICMPv4** oder **ICMPv6** aus. Wenn Sie IPv4 und IPv6 in Ihrem Netzwerk verwenden, müssen Sie für jede eine separate ICMP-Regel erstellen.
7. Klicken Sie auf **Anpassen**.
8. Führen Sie im Dialogfeld **ICMP-Einstellungen anpassen** eine der folgenden Aktionen aus:
   - Wenn Sie den gesamten ICMP-Netzwerkdatenverkehr zulassen möchten, klicken Sie auf **alle ICMP-Typen**, und klicken Sie dann auf **OK**.
   - Wenn Sie einen der vordefinierten ICMP-Typen auswählen möchten, klicken Sie auf **bestimmte ICMP-Typen**, und wählen Sie dann die einzelnen Typen in der Liste aus, die Sie zulassen möchten. Klicken Sie auf **OK**.
   - Wenn Sie einen ICMP-Typ auswählen möchten, der nicht in der Liste angezeigt wird, klicken Sie auf **bestimmte ICMP-Typen**, wählen Sie die Nummer des **Typs** aus der Liste aus, wählen Sie die

Code Nummer aus der Liste aus, klicken Sie auf **Hinzufügen**, und wählen Sie dann den neu erstellten Eintrag aus der Liste aus. Klicken Sie auf **OK**.

9. Klicken Sie auf **Weiter**.
10. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.
11. Wählen Sie **** auf der Seite Aktion **die Option Verbindung zulassen**aus, und klicken Sie dann auf **weiter**.
12. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.
13. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen einer Porteingangsregel

10.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie eingehenden Netzwerkdatenverkehr nur für eine bestimmte TCP-oder UDP-Portnummer zulassen möchten, verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit im MMC-Snap-in Gruppenrichtlinienverwaltung, um Firewallregeln zu erstellen. Dieser Regeltyp ermöglicht es jedem Programm, das einen angegebenen TCP-oder UDP-Port überwacht, den an diesen Port gesendeten Netzwerkdatenverkehr zu empfangen.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

In diesem Thema wird beschrieben, wie Sie eine Standardportregel für ein bestimmtes Protokoll oder eine TCP-oder UDP-Portnummer erstellen. Informationen zu anderen Regeltypen für eingehende Ports finden Sie unter:

- Erstellen einer ICMP-Eingangsregel
- Erstellen von Eingangsregeln zur RPC-Unterstützung

So erstellen Sie eine eingehende Portregel

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Eingehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.

   > **Hinweis:** Obwohl Sie Regeln erstellen können, indem Sie **Programm** oder **Port**auswählen, begrenzen diese Auswahlmöglichkeiten die Anzahl der Seiten, die vom Assistenten angezeigt werden. Wenn Sie **Benutzerdefiniert**auswählen, werden alle Seiten angezeigt, und Sie haben die größte Flexibilität beim Erstellen von Regeln.

5. Klicken Sie auf der Seite **Programm** auf **Alle Programme**, und klicken Sie dann auf **weiter**.

   > **Hinweis:** Diese Art von Regel wird häufig mit einer Programm-oder Dienst Regel kombiniert. Wenn Sie die Regeltypen kombinieren, erhalten Sie eine Firewall-Regel, die den Datenverkehr auf einen angegebenen Port beschränkt und den Datenverkehr nur dann zulässt, wenn das angegebene Programm ausgeführt wird. Das angegebene Programm kann keinen Netzwerkdatenverkehr auf anderen Ports empfangen, und andere Programme können keinen Netzwerkdatenverkehr am angegebenen Port empfangen. Wenn Sie sich dafür entscheiden, führen Sie die Schritte im Verfahren zum Erstellen eines eingehenden Programms oder einer Dienst Regel zusätzlich zu den Schritten in diesem Verfahren aus, um eine einzelne Regel zu erstellen, die den Netzwerkdatenverkehr mithilfe von Programm-und Port Kriterien filtert.

6. Wählen Sie auf der Seite **Protokoll und Ports** den Protokolltyp aus, den Sie zulassen möchten. Wenn Sie die Regel auf eine bestimmte Portnummer einschränken möchten, müssen Sie entweder **TCP** oder **UDP**auswählen. Da es sich um eine eingehende Regel handelt, konfigurieren Sie in der Regel nur die lokale Portnummer.

   Wenn Sie ein anderes Protokoll auswählen, werden nur Pakete, deren Protokollfeld im IP-Header dieser Regel entspricht, über die Firewall zugelassen.

   Wenn Sie ein Protokoll anhand seiner Nummer auswählen möchten, wählen Sie in der Liste **Benutzerdefiniert** aus, und geben Sie dann die Nummer in das Feld **Protokollnummer** ein.

   Wenn Sie die Protokolle und Ports konfiguriert haben, klicken Sie auf **weiter**.

7. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.

8. Wählen Sie **** auf der Seite Aktion **die Option Verbindung zulassen**aus, und klicken Sie dann auf **weiter**.

9. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.

   > **Hinweis:** Wenn dieses Gruppenrichtlinienobjekt auf Server Computern mit Windows Server 2008 ausgerichtet ist, die sich nie bewegen, sollten Sie die Regeln so ändern, dass Sie auf alle Profile des Netzwerkstandorttyps angewendet werden. Dadurch wird eine unerwartete Änderung der angewendeten Regeln verhindert, wenn sich der Typ des Netzwerkstandorts aufgrund der Installation einer neuen Netzwerkkarte oder der Trennung des Kabels einer vorhandenen Netzwerkkarte ändert. Eine getrennte Netzwerkkarte wird dem Standorttyp des öffentlichen Netzwerks automatisch zugewiesen.

10. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen einer Programm- oder Diensteingangsregel

01.06.2019 • 4 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Um eingehenden Netzwerkdatenverkehr an ein bestimmtes Programm oder einen bestimmten Dienst zu ermöglichen, verwenden Sie die Windows Defender-Firewall mit erweitertem Securitynode im MMC-Snap-in Gruppenrichtlinienverwaltung, um Firewallregeln zu erstellen. Dieser Regeltyp ermöglicht es dem Programm, eingehenden Netzwerkdatenverkehr an einem beliebigen Port zu überwachen und zu empfangen.

> **Hinweis:** diese Art von Regel wird häufig mit einer Programm-oder Dienst Regel kombiniert. Wenn Sie die Regeltypen kombinieren, erhalten Sie eine Firewall-Regel, die den Datenverkehr auf einen angegebenen Port beschränkt und den Datenverkehr nur dann zulässt, wenn das angegebene Programm ausgeführt wird. Das Programm kann keinen Netzwerkdatenverkehr auf anderen Ports empfangen, und andere Programme können keinen Netzwerkdatenverkehr am angegebenen Port empfangen. Wenn Sie die Programm-und Port Regeltypen in einer einzigen Regel kombinieren möchten, führen Sie die Schritte im Verfahren zum Erstellen einer eingehenden Port Regel zusätzlich zu den Schritten in diesem Verfahren aus.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So erstellen Sie eine eingehende Firewall-Regel für ein Programm oder einen Dienst

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Eingehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.

   > **Hinweis:** obwohl Sie Regeln erstellen können, indem Sie **Programm** oder **Port**auswählen, begrenzen diese Auswahlmöglichkeiten die Anzahl der Seiten, die vom Assistenten angezeigt werden. Wenn Sie **Benutzerdefiniert**auswählen, werden alle Seiten angezeigt, und Sie haben die größte Flexibilität beim Erstellen von Regeln.

5. Klicken Sie auf der Seite **Programm** auf **diesen Programmpfad**.
6. Geben Sie den Pfad zu dem Programm in das Textfeld ein. Verwenden Sie ggf. Umgebungsvariablen, um sicherzustellen, dass Programme, die an verschiedenen Speicherorten auf unterschiedlichen Computern installiert sind, ordnungsgemäß funktionieren.
7. Führen Sie einen der folgenden Schritte aus:
   - Wenn die ausführbare Datei ein einzelnes Programm enthält, klicken Sie auf **weiter**.

- Wenn es sich bei der ausführbaren Datei um einen Container für mehrere Dienste handelt, bei denen alle eingehenden Netzwerkdatenverkehr empfangen dürfen, klicken Sie auf **Anpassen**, wählen Sie **nur auf Dienste anwenden**aus, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
- Wenn es sich bei der ausführbaren Datei um einen Container für einen einzelnen Dienst oder um mehrere Dienste handelt, die Regel aber nur für eine dieser Dienste gilt, klicken Sie auf **Anpassen**, wählen Sie für **diesen Dienst übernehmen**aus, und wählen Sie dann den Dienst in der Liste aus. Wenn der Dienst nicht in der Liste angezeigt wird, klicken Sie auf **für Dienst mit diesem Dienstkurznamen übernehmen**, und geben Sie dann den kurzen Namen für den Dienst in das Textfeld ein. Klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.

Wichtig Wenn Sie die Optionen **für diesen Dienst anwenden** oder **auf Dienst anwenden mit diesem Dienst** verwenden möchten, muss der Dienst mit einer Sicherheits-ID (Security Identifier, SID) mit einem **eingeschränkten** oder uneingeschränkten Typ konfiguriert werden. **** Führen Sie den folgenden Befehl aus, um den SID-Typ eines Diensts zu überprüfen:

SC qsidtype * <Dienstname> *

Wenn das Ergebnis **keine**ist, kann keine Firewall-Regel auf diesen Dienst angewendet werden.

Führen Sie den folgenden Befehl aus, um einen SID-Typ für einen Dienst einzurichten:

SC SIDType *Geben>Sie ServiceName>* <<

Im vorhergehenden Befehl kann der Wert * <vom> Typ* **Unrestricted** oder **eingeschränkt**sein. Obwohl der Befehl auch den Wert **None**zulässt, bedeutet diese Einstellung, dass der Dienst in einer Firewallregel wie hier beschrieben nicht verwendet werden kann. Standardmäßig sind die meisten Dienste in Windows als " **unbeschränkt**" konfiguriert. Wenn Sie den SID-Typ in **restricted**ändern, kann der Dienst möglicherweise nicht gestartet werden. Wir empfehlen, dass Sie den SID-Typ nur für Dienste ändern, die Sie in Firewallregeln verwenden möchten, und dass Sie den SID-Typ in **Unrestricted**ändern.

8. Es empfiehlt sich, die Firewall-Regel für das Programm auf die Ports zu beschränken, die für den Betrieb benötigt werden. Auf der Seite **Protokolle und Ports** können Sie die Portnummern für den zulässigen Datenverkehr angeben. Wenn das Programm versucht, einen anderen als den hier angegebenen Port abzuhören, ist es blockiert. Weitere Informationen zu Protokoll-und Portoptionen finden Sie unter Erstellen einer eingehenden Port Regel. Nachdem Sie die Optionen für Protokoll und Port konfiguriert haben, klicken Sie auf **weiter**.
9. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.
10. Wählen Sie **** auf der Seite Aktion **die Option Verbindung zulassen**aus, und klicken Sie dann auf **weiter**.
11. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.
12. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen einer Portausgangsregel

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Standardmäßig lässt die Windows Defender-Firewall alle ausgehenden Netzwerkdatenverkehr zu, es sei denn, Sie entspricht einer Regel, die den Datenverkehr verbietet. Zum Blockieren des ausgehenden Netzwerkverkehrs an einer bestimmten TCP-oder UDP-Portnummer verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit in der Gruppenrichtlinien-Verwaltungskonsole, um Firewallregeln zu erstellen. Diese Art von Regel blockiert ausgehenden Netzwerkdatenverkehr, der den angegebenen TCP-oder UDP-Portnummern entspricht.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So erstellen Sie eine ausgehende Port Regel

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **ausgehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue ausgehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.

   > **Hinweis:** obwohl Sie Regeln erstellen können, indem Sie **Programm** oder **Port**auswählen, begrenzen diese Auswahlmöglichkeiten die Anzahl der Seiten, die vom Assistenten angezeigt werden. Wenn Sie **Benutzerdefiniert**auswählen, werden alle Seiten angezeigt, und Sie haben die größte Flexibilität beim Erstellen von Regeln.

5. Klicken Sie auf der Seite **Programm** auf **Alle Programme**, und klicken Sie dann auf **weiter**.
6. Wählen Sie auf der Seite **Protokoll und Ports** den Protokolltyp aus, den Sie blockieren möchten. Wenn Sie die Regel auf eine bestimmte Portnummer einschränken möchten, müssen Sie entweder **TCP** oder **UDP**auswählen. Da es sich um eine ausgehende Regel handelt, konfigurieren Sie in der Regel nur die Remoteportnummer.

   Wenn Sie ein anderes Protokoll auswählen, werden nur Pakete, deren Protokollfeld im IP-Header dieser Regel entspricht, von der Windows Defender-Firewall blockiert. Netzwerkdatenverkehr für Protokolle ist zulässig, solange andere Regeln, die übereinstimmen, ihn nicht blockieren.

   Wenn Sie ein Protokoll anhand seiner Nummer auswählen möchten, wählen Sie in der Liste **Benutzerdefiniert** aus, und geben Sie dann die Nummer in das Feld **Protokollnummer** ein.

   Wenn Sie die Protokolle und Ports konfiguriert haben, klicken Sie auf **weiter**.
7. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von

den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.

8. Wählen Sie **** auf der Seite Aktion **die Option Verbindung blockieren**aus, und klicken Sie dann auf **weiter**.
9. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.
10. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen einer Programm- oder Dienstausgangsregel

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Standardmäßig lässt die Windows Defender-Firewall alle ausgehenden Netzwerkdatenverkehr zu, es sei denn, Sie entspricht einer Regel, die den Datenverkehr verbietet. Um ausgehenden Netzwerkdatenverkehr für ein bestimmtes Programm oder einen bestimmten Dienst zu blockieren, verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit in der Gruppenrichtlinien-Verwaltungskonsole, um Firewallregeln zu erstellen. Diese Art von Regel verhindert, dass das Programm ausgehenden Netzwerkdatenverkehr an einem beliebigen Port sendet.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So erstellen Sie eine ausgehende Firewall-Regel für ein Programm oder einen Dienst

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **ausgehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue ausgehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.

   > **Hinweis:** obwohl Sie viele Regeln erstellen können, indem Sie **Programm** oder **Port**auswählen, begrenzen diese Auswahlmöglichkeiten die Anzahl der Seiten, die vom Assistenten angezeigt werden. Wenn Sie **Benutzerdefiniert**auswählen, werden alle Seiten angezeigt, und Sie haben die größte Flexibilität beim Erstellen von Regeln.

5. Klicken Sie auf der Seite **Programm** auf **diesen Programmpfad**.
6. Geben Sie den Pfad zu dem Programm in das Textfeld ein. Verwenden Sie Umgebungsvariablen, um sicherzustellen, dass Programme, die an verschiedenen Speicherorten auf unterschiedlichen Computern installiert sind, ordnungsgemäß funktionieren.
7. Führen Sie einen der folgenden Schritte aus:

   - Wenn die ausführbare Datei ein einzelnes Programm enthält, klicken Sie auf **weiter**.
   - Wenn es sich bei der ausführbaren Datei um einen Container für mehrere Dienste handelt, die alle daran gehindert werden müssen, ausgehenden Netzwerkdatenverkehr zu senden, klicken Sie auf **Anpassen**, wählen Sie **nur auf Dienste anwenden**aus, klicken Sie auf **OK**und dann auf **weiter**.
   - Wenn es sich bei der ausführbaren Datei um einen Container für einen einzelnen Dienst oder um mehrere Dienste handelt, die Regel aber nur für eine dieser Dienste gilt, klicken Sie auf **Anpassen**, wählen Sie für **diesen Dienst übernehmen**aus, und wählen Sie dann den Dienst in der Liste aus.

Wenn der Dienst nicht in der Liste angezeigt wird, klicken Sie auf **für Dienst mit diesem Dienstkurznamen übernehmen**, und geben Sie den kurzen Namen für den Dienst in das Textfeld ein. Klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.

8. Wenn Sie möchten, dass das Programm auf einigen Ports senden, aber nicht an andere senden kann, können Sie die Firewallregel so einschränken, dass nur die angegebenen Ports oder Protokolle blockiert werden. Auf der Seite **Protokolle und Ports** können Sie die Portnummern oder Protokollnummern für den blockierten Datenverkehr angeben. Wenn das Programm versucht, eine von der hier angegebenen Portnummer zu senden oder eine andere als die hier angegebene Protokollnummer zu verwenden, kann das Standardverhalten der ausgehenden Firewall den Datenverkehr übernehmen. Weitere Informationen zu den Protokoll-und Portoptionen finden Sie unter Erstellen einer ausgehenden Port Regel. Wenn Sie die Optionen Protokoll und Port konfiguriert haben, klicken Sie auf **weiter**.

9. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.

10. Wählen Sie **** auf der Seite Aktion **die Option Verbindung blockieren**aus, und klicken Sie dann auf **weiter**.

11. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.

12. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen von Eingangsregeln zur RPC-Unterstützung

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Zum Zulassen des eingehenden RPC-Netzwerkverkehrs (Remote Procedure Call) verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit in der Gruppenrichtlinien-Verwaltungskonsole, um zwei Firewallregeln zu erstellen. Die erste Regel ermöglicht eingehende Netzwerkpakete am TCP-Port 135 an den RPC-Endpunktzuordnungsdienst. Der eingehende Datenverkehr besteht aus Anforderungen an die Kommunikation mit einem angegebenen Netzwerkdienst. Die RPC-Endpunktzuordnung beantwortet eine dynamisch zugewiesene Portnummer, die der Client für die Kommunikation mit dem Dienst verwenden muss. Die zweite Regel ermöglicht den Netzwerkdatenverkehr, der an die dynamisch zugewiesene Portnummer gesendet wird. Mit den beiden in diesem Thema beschriebenen Regeln können Sie Ihr Gerät schützen, indem Sie den Netzwerkdatenverkehr nur von Geräten zulassen, die eine dynamische RPC-Portumleitung erhalten haben, und nur für die von der RPC-Endpunktzuordnung zugewiesenen TCP-Portnummern.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

In diesem Thema wird beschrieben, wie Regeln erstellt werden, die eingehenden RPC-Netzwerkdatenverkehr ermöglichen. Informationen zu anderen Regeltypen für eingehende Ports finden Sie unter:

- Erstellen einer Porteingangsregel
- Erstellen einer ICMP-Eingangsregel

In diesem Thema:

So erstellen Sie eine Regel zum Zulassen des eingehenden Netzwerkverkehrs an den RPC-Endpunktzuordnungsdienst

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Eingehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.
5. Klicken Sie auf der Seite **Programm** auf **diesen Programmpfad**, und geben Sie dann **%systemroot%\system32\svchost.exe**ein.

6. Klicken Sie auf **Anpassen**.
7. Klicken Sie im Dialogfeld **Diensteinstellungen anpassen** auf **für diesen Dienst übernehmen**, wählen Sie **Remote Prozeduraufruf (Remote Procedure Call, RPC)** mit einem kurzen Namen von **RPCSS**aus, klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
8. Klicken Sie in der Warnung zu Windows-Dienst Härtungs Regeln auf **Ja**.
9. Wählen Sie im Dialogfeld **Protokoll und Ports** für **Protokolltyp**die Option **TCP**aus.
10. Wählen Sie für **lokaler Port RPC-Endpunktzuordnung**aus, und klicken Sie dann auf **weiter**.
11. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.
12. Wählen Sie **** auf der Seite Aktion **die Option Verbindung zulassen**aus, und klicken Sie dann auf **weiter**.
13. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.
14. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

So erstellen Sie eine Regel zum Zulassen des eingehenden Netzwerkverkehrs an RPC-fähige Netzwerkdienste

1. Klicken Sie in demselben GPO, das Sie im vorherigen Verfahren bearbeitet haben, auf **Aktion**und dann auf **neue Regel**.
2. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.
3. Klicken Sie auf der Seite **Programm** auf **diesen Programmpfad**, und geben Sie dann den Pfad zu der ausführbaren Datei ein, die den Netzwerkdienst hostet. Klicken Sie auf **Anpassen**.
4. Klicken Sie im Dialogfeld **Diensteinstellungen anpassen** auf **für diesen Dienst übernehmen**, und wählen Sie dann den Dienst aus, den Sie zulassen möchten. Wenn der Dienst nicht in der Liste angezeigt wird, klicken Sie auf **für Dienst mit diesem Dienstkurznamen übernehmen**, und geben Sie dann den kurzen Namen des Diensts in das Textfeld ein.
5. Klicken Sie auf **OK**, und klicken Sie dann auf **weiter**.
6. Wählen Sie im Dialogfeld **Protokoll und Ports** für **Protokolltyp**die Option **TCP**aus.
7. Wählen Sie für **lokaler Port RPC Dynamic Ports**aus, und klicken Sie dann auf **weiter**.
8. Auf der Seite " **Bereich** " können Sie angeben, dass die Regel nur für den Netzwerkverkehr zu oder von den auf dieser Seite eingegebenen IP-Adressen gelten soll. Konfigurieren Sie die für Ihr Design geeignete Konfiguration, und klicken Sie dann auf **weiter**.
9. Wählen Sie **** auf der Seite Aktion **die Option Verbindung zulassen**aus, und klicken Sie dann auf **weiter**.
10. Wählen Sie auf der Seite **Profil** die Netzwerkadresstypen aus, für die diese Regel gilt, und klicken Sie dann auf **weiter**.
11. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für die Regel ein, und klicken Sie dann auf **Fertig stellen**.

Erstellen von WMI-Filtern für Gruppenrichtlinienobjekte

11.10.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Wenn Sie sicherstellen möchten, dass jedes Gruppenrichtlinienobjekt, das einer Gruppe zugeordnet ist, nur auf Geräte angewendet werden kann, auf denen die richtige Version von Windows ausgeführt wird, verwenden Sie das MMC-Snap-in Gruppenrichtlinienverwaltung, um dem GPO WMI-Filter zu erstellen und zuzuweisen. Obwohl Sie für jedes GPO eine separate Mitgliedschaftsgruppe erstellen können, müssen Sie die Mitgliedschaften der verschiedenen Gruppen verwalten. Verwenden Sie stattdessen nur eine einzige Mitgliedschaftsgruppe, und lassen Sie WMI-Filter automatisch sicherstellen, dass das richtige Gruppenrichtlinienobjekt auf jedes Gerät angewendet wird.

- So erstellen Sie einen WMI-Filter, der eine bestimmte Version von Windows abfragt
- So verknüpfen Sie einen WMI-Filter mit einem Gruppenrichtlinienobjekt

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

Erstellen Sie zunächst den WMI-Filter, und konfigurieren Sie ihn so, dass er nach einer bestimmten Version (oder Versionen) des Windows-Betriebssystems sucht.

So erstellen Sie einen WMI-Filter, der eine bestimmte Version von Windows abfragt

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:** *YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, und klicken Sie dann auf **WMI-Filter**.
3. Klicken Sie auf **Aktion**und dann auf **neu**.
4. Geben Sie im Textfeld **Name** den Namen des WMI-Filters ein.

   > **Hinweis:** verwenden Sie unbedingt einen Namen, der den Zweck des Filters eindeutig angibt. Überprüfen Sie, ob Ihre Organisation über eine Benennungskonvention verfügt.

5. Geben Sie im Textfeld **Beschreibung** eine Beschreibung für den WMI-Filter ein. Wenn der Filter beispielsweise Domänencontroller ausschließt, sollten Sie dies in der Beschreibung angeben.
6. Klicken Sie auf **Hinzufügen**.
7. Belasse den **Namespace** -Wert auf **root\CIMv2**.
8. Geben Sie im Textfeld **Abfrage** Folgendes ein:

```
select * from Win32_OperatingSystem where Version like "6.%"
```

Diese Abfrage gibt **true** für Geräte zurück, auf denen mindestens Windows Vista und Windows Server2008 ausgeführt werden. Verwenden Sie "6,2%", um einen Filter für Windows 8 und Windows Server 2012 einzurichten. Verwenden Sie für Windows 10 und Windows Server 2016 "10.%". Wenn Sie mehrere Versionen angeben möchten, kombinieren Sie Sie mit oder, wie in der folgenden Abbildung dargestellt:

```
... where Version like "6.1%" or Version like "6.2%"
```

Wenn Sie die Abfrage nur auf Clients oder nur auf Server einschränken möchten, fügen Sie eine Klausel hinzu, die den ProductType-Parameter enthält. Wenn Sie nur nach Clientbetriebssystemen wie Windows 8 oder Windows7 filtern möchten, verwenden Sie nur ProductType = "1". Bei Server Betriebssystemen, bei denen es sich nicht um Domänencontroller handelt, verwenden Sie ProductType = "3". Verwenden Sie bei Domänencontrollern nur ProductType = "2". Dies ist eine nützliche Unterscheidung, da Sie häufig verhindern möchten, dass Ihre GPOs auf die Domänencontroller in Ihrem Netzwerk angewendet werden.

Die folgende Klausel gibt für alle Geräte, die keine Domänencontroller sind, " **true** " zurück:

```
... where ProductType="1" or ProductType="3"
```

Die folgende vollständige Abfrage gibt für alle Geräte, auf denen Windows 10 ausgeführt wird, **true** zurück, und gibt für alle Server Betriebssysteme oder andere Clientbetriebssysteme **false** zurück.

```
select * from Win32_OperatingSystem where Version like "10.%" and ProductType="1"
```

Mit der folgenden Abfrage wird für jedes Gerät, auf dem Windows Server 2016 ausgeführt wird, mit Ausnahme von Domänencontrollern **true** zurückgegeben:

```
select * from Win32_OperatingSystem where Version like "10.%" and ProductType="3"
```

9. Klicken Sie auf **OK** , um die Abfrage im Filter zu speichern.
10. Klicken Sie auf **Speichern** , um den abgeschlossenen Filter zu speichern.

> **NOTE**
> Wenn Sie mehrere Abfragen im gleichen WMI-Filter verwenden, müssen diese Abfragen alle **true** zurückgeben, damit die Filteranforderungen erfüllt werden, und das Gruppenrichtlinienobjekt angewendet werden.

So verknüpfen Sie einen WMI-Filter mit einem Gruppenrichtlinienobjekt

Nachdem Sie einen Filter mit der richtigen Abfrage erstellt haben, verknüpfen Sie den Filter mit dem Gruppenrichtlinienobjekt. Filter können gleichzeitig mit vielen GPOs wieder verwendet werden. Sie müssen für jedes GPO keine neue erstellen, wenn eine vorhandene Person Ihren Anforderungen entspricht.

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Suchen Sie im Navigationsbereich, und klicken Sie dann auf das Gruppenrichtlinienobjekt, das Sie ändern möchten.

3. Wählen Sie unter **WMI-Filterung**den richtigen WMI-Filter aus der Liste aus.

4. Klicken Sie auf **Ja** , um den Filter zu akzeptieren.

Erstellen von Windows-Firewallregeln in InTune

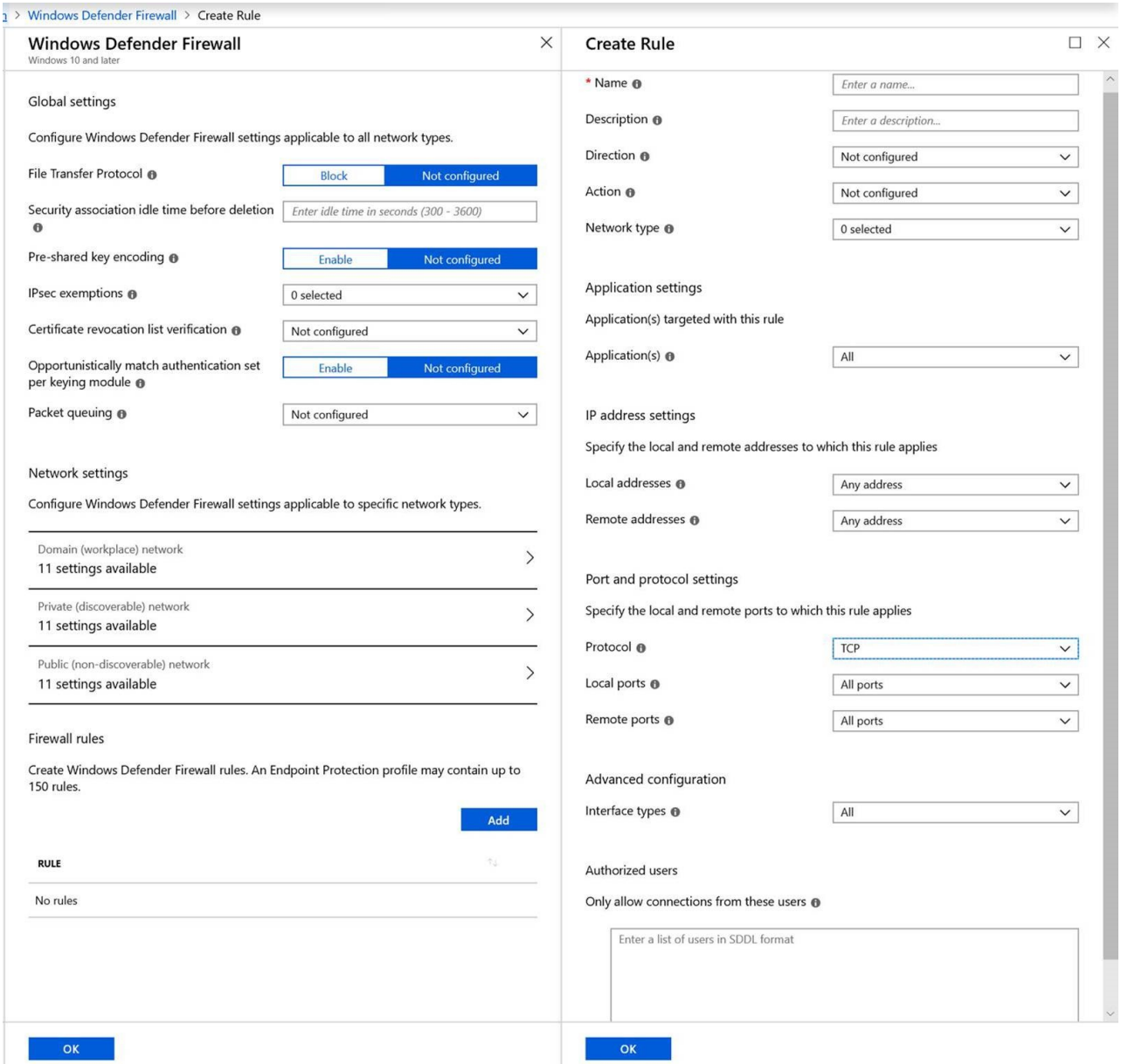
11.10.2019 • 3 minutes to read

Betrifft

- Windows 10

> **IMPORTANT**
> Diese Informationen beziehen sich auf vorab veröffentlichte Produkte, die vor der kommerziellen Veröffentlichung erheblich geändert werden können. Microsoft übernimmt keine Garantie, weder ausdrücklich noch stillschweigend, für die hier bereitgestellten Informationen.

Öffnen Sie zunächst die Gerätekonfiguration in InTune, und erstellen Sie dann ein neues Profil. Wählen Sie Windows 10 als Plattform und Endpunktschutz als Profiltyp aus. Wählen Sie Windows Defender Firewall aus.



IMPORTANT

Ein einzelnes Endpunktschutz Profil kann bis zu maximal 150 Firewall-Regeln enthalten. Wenn für ein Clientgerät mehr als 150-Regeln erforderlich sind, müssen ihm mehrere Profile zugewiesen werden.

Firewall-Regelkomponenten

Die Firewall-Regel Konfigurationen in InTune verwenden den Windows 10-CSP für Firewall. Weitere Informationen finden Sie unter Firewall-CSP.

Application

Steuern von Verbindungen für eine APP oder ein Programm Apps und Programme können entweder Dateipfad, Paket Familienname oder Windows Service Short Name angegeben werden.

Der Dateipfad einer APP ist die Position auf dem Clientgerät. Beispiel: C:\Windows\System\Notepad.exe. Weitere Informationen

Paket Familiennamen können abgerufen werden, indem Sie den Befehl Get-AppxPackage aus PowerShell ausführen. Weitere Informationen

Kurz Namen für Windows-Dienste werden in Fällen verwendet, in denen ein Dienst, keine Anwendung, Datenverkehr sendet oder empfängt. Standard IA alle.

Weitere Informationen

Protokoll

Wählen Sie das Protokoll für diese Port Regel aus. Über Transport Schichtprotokolle – TCP und UDP – können Sie Ports oder Portbereiche angeben. Geben Sie für benutzerdefinierte Protokolle eine Zahl zwischen 0 und 255 ein, die das IP-Protokoll darstellt.

Standard ist any.

Weitere Informationen

Lokale Anschlüsse

Durch trennzeichengetrennte Liste von Bereichen. Beispiel: *100-120200300-320*. Standard ist alle.

Weitere Informationen

Remote Anschlüsse

Durch trennzeichengetrennte Liste von Bereichen. Beispiel: *100-120200300-320*. Standard ist alle.

Weitere Informationen

Lokale Adressen

Durch trennzeichengetrennte Liste der lokalen Adressen, die unter die Regel fallen. Gültige Token sind:

- \ * gibt eine lokale Adresse an. Wenn vorhanden, muss dies das einzige Token sein, das enthalten ist.
- Ein Subnetz kann entweder mithilfe der Subnetzmaske oder der Netzwerkpräfix Notation angegeben werden. Wenn weder eine Subnetzmaske noch ein Netzwerkpräfix angegeben ist, ist die Subnetzmaske standardmäßig 255.255.255.255.

- Eine gültige IPv6-Adresse.
- Ein IPv4-Adressbereich im Format "Start address-End Address" ohne Leerzeichen.
- Ein IPv6-Adressbereich im Format "Start address-End Address" ohne Leerzeichen. Standard ist eine beliebige Adresse.

Weitere Informationen

Remote Adressen

Liste der durch Kommas getrennten Token, die die von der Regel abgedeckten Remoteadressen angeben. Bei Token wird die Groß-/Kleinschreibung nicht berücksichtigt. Gültige Token sind:

- \ * gibt eine beliebige Remoteadresse an. Wenn vorhanden, muss dies das einzige Token sein, das enthalten ist.
- DefaultGateway
- DHCP
- DNS
- Gewinnt
- Intranet (unter Windows-Versionen 1809 + unterstützt)
- RmtIntranet (unter Windows-Versionen 1809 +)
- Internet (unter Windows-Versionen 1809 +)
- Ply2Renders (unter Windows-Versionen 1809 +)
- LocalSubnet gibt eine beliebige lokale Adresse im lokalen Subnetz an.
- Ein Subnetz kann entweder mithilfe der Subnetzmaske oder der Netzwerkpräfix Notation angegeben werden. Wenn weder eine Subnetzmaske noch ein Netzwerkpräfix angegeben ist, ist die Subnet-Maske standardmäßig 255.255.255.255.
- Eine gültige IPv6-Adresse.
- Ein IPv4-Adressbereich im Format "Start address-End Address" ohne Leerzeichen.
- Ein IPv6-Adressbereich im Format "Start address-End Address" ohne Leerzeichen.

Standard ist eine beliebige Adresse.

Weitere Informationen

Edge-Traversal (UI in Kürze verfügbar)

Gibt an, ob der Edge-Traversal für diese Regel aktiviert oder deaktiviert ist. Die Einstellung "EdgeTraversal" gibt an, dass ein bestimmter eingehender Datenverkehr mithilfe der Teredo-Tunneltechnologie durch NATs und andere Edge-Geräte Tunneln darf. Damit diese Einstellung ordnungsgemäß funktioniert, muss die Anwendung oder der Dienst mit der Regel für eingehende Firewalls IPv6 unterstützen. Die primäre Anwendung dieser Einstellung ermöglicht es den Listenern auf dem Host, über eine Teredo-IPv6-Adresse global adressierbar zu sein. Bei neuen Regeln ist die EdgeTraversal-Eigenschaft standardmäßig deaktiviert. Diese Einstellung kann zu diesem Zeitpunkt nur über InTune-Diagramm konfiguriert werden.

Weitere Informationen

Autorisierte Benutzer

Gibt die Liste der autorisierten lokalen Benutzer für diese Regel an. Eine Liste der autorisierten Benutzer kann nicht angegeben werden, wenn die zu verfassende Regel auf einen Windows-Dienst ausgerichtet ist. Standard ist "alle Benutzer".

Weitere Informationen

Programmgesteuertes Konfigurieren von Firewallregeln

Bald verfügbar.

Aktivieren von vordefinierten Eingangsregeln

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die Windows Defender-Firewall mit erweiterter Sicherheit umfasst viele vordefinierte Regeln für allgemeine Netzwerk Rollen und-Funktionen. Wenn Sie eine neue Serverrolle auf einem Gerät installieren oder ein Netzwerkfeature auf einem Clientgerät aktivieren, ermöglicht das Installationsprogramm in der Regel die für diese Rolle erforderlichen Regeln, anstatt neue zu erstellen. Wenn Sie Firewallregeln für die Geräte im Netzwerk bereitstellen, können Sie diese vordefinierten Regeln nutzen, anstatt neue zu erstellen. Auf diese Weise können Sie Konsistenz und Genauigkeit gewährleisten, da die Regeln gründlich getestet wurden und einsatzbereit sind.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So stellen Sie vordefinierte Firewallregeln bereit, die eingehenden Netzwerkdatenverkehr für allgemeine Netzwerkfunktionen zulassen

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **Eingehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **vordefiniert**, wählen Sie die Regelkategorie in der Liste aus, und klicken Sie dann auf **weiter**.
5. Auf der Seite vordefinierte **Regeln** wird die Liste der in der Gruppe definierten Regeln angezeigt. Standardmäßig sind Sie alle ausgewählt. Deaktivieren Sie für Regeln, die Sie nicht bereitstellen möchten, die Kontrollkästchen neben den Regeln, und klicken Sie dann auf **weiter**.
6. Wählen Sie **** auf der Seite Aktion **die Option Verbindung zulassen**aus, und klicken Sie dann auf **Fertig stellen**.

Aktivieren von vordefinierten Ausgangsregeln

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Standardmäßig ermöglicht die Windows Defender-Firewall mit erweiterter Sicherheit allen ausgehenden Netzwerkdatenverkehr, es sei denn, Sie entspricht einer Regel, die den Datenverkehr verbietet. Die Windows Defender-Firewall enthält viele vordefinierte ausgehende Regeln, die zum Blockieren des Netzwerkverkehrs für allgemeine Netzwerk Rollen und-Funktionen verwendet werden können. Wenn Sie eine neue Serverrolle auf einem Computer installieren oder ein Netzwerkfeature auf einem Clientcomputer aktivieren, kann das Installationsprogramm installieren, aber in der Regel keine ausgehenden Blockierungsregeln für diese Rolle aktivieren. Wenn Sie Firewallregeln auf den Computern im Netzwerk bereitstellen, können Sie diese vordefinierten Regeln nutzen, anstatt neue zu erstellen. Auf diese Weise können Sie Konsistenz und Genauigkeit gewährleisten, da die Regeln gründlich getestet wurden und einsatzbereit sind.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So stellen Sie vordefinierte Firewallregeln bereit, die ausgehenden Netzwerkdatenverkehr für allgemeine Netzwerkfunktionen blockieren

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Navigationsbereich auf **ausgehende Regeln**.
3. Klicken Sie auf **Aktion**und dann auf **neue Regel**.
4. Klicken Sie **** auf der Seite Regeltyp des Assistenten für neue eingehende Regel auf **vordefiniert**, wählen Sie die Regelkategorie in der Liste aus, und klicken Sie dann auf **weiter**.
5. Auf der Seite vordefinierte **Regeln** wird die Liste der in der Gruppe definierten Regeln angezeigt. Sie sind standardmäßig ausgewählt. Deaktivieren Sie für Regeln, die Sie nicht bereitstellen möchten, die Kontrollkästchen neben den Regeln, und klicken Sie dann auf **weiter**.
6. Wählen Sie **** auf der Seite Aktion **die Option Verbindung blockieren**aus, und klicken Sie dann auf **Fertig stellen**.

   Die ausgewählten Regeln werden dem Gruppenrichtlinienobjekt hinzugefügt.

Ausschließen von ICMP aus der Authentifizierung

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Verfahren wird gezeigt, wie Ausnahmen für Netzwerkdatenverkehr hinzugefügt werden, der das ICMP-Protokoll verwendet.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über die Berechtigung zum Ändern der GPOs verfügen.

So nehmen Sie den ICMP-Netzwerkdatenverkehr von der Authentifizierung frei

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie auf der Hauptseite der Windows Defender-Firewall mit erweiterter Sicherheit auf **Windows Defender-Firewall-Eigenschaften**.
3. Ändern Sie auf der Registerkarte **IPSec-Einstellungen** die **Ausnahme ICMP von IPSec** auf **Ja**, und klicken Sie dann auf **OK**.

Verknüpfen des Gruppenrichtlinienobjekts mit der Domäne

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie das Gruppenrichtlinienobjekt erstellt und mit Sicherheitsgruppen Filtern und WMI-Filtern konfiguriert haben, müssen Sie das Gruppenrichtlinienobjekt mit dem Container in Active Directory verknüpfen, in dem alle Zielgeräte enthalten sind.

Wenn die Filter die Anwendung des Gruppenrichtlinienobjekts auf die richtigen Geräte umfassend steuern, können Sie das Gruppenrichtlinienobjekt mit dem Domänencontainer verknüpfen. Alternativ können Sie das Gruppenrichtlinienobjekt mit einem Website Container oder einer Organisationseinheit verknüpfen, wenn Sie die Anwendung des Gruppenrichtlinienobjekts auf diese Teilmenge von Geräten einschränken möchten.

Administrative Anmeldeinformationen

Um dieses Verfahren ausführen zu können, müssen Sie Mitglied der Gruppe der Domänenadministratoren sein oder auf andere Weise über die Berechtigung zum Ändern der GPOs verfügen.

So verknüpfen Sie das Gruppenrichtlinienobjekt mit dem Domänencontainer in Active Directory

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:** *YourForestName*, erweitern Sie **Domänen**, und erweitern Sie dann *IhrDomänenname*.
3. Klicken Sie mit der rechten Maustaste auf *IhrDomänenname*, und klicken Sie dann auf **vorhandenes Gruppenrichtlinienobjekt verknüpfen**.
4. Wählen Sie im Dialogfeld **GPO auswählen** das Gruppenrichtlinienobjekt aus, das Sie bereitstellen möchten, und klicken Sie dann auf **OK**.
5. Das Gruppenrichtlinienobjekt wird auf der Registerkarte **verknüpfte Gruppenrichtlinienobjekte** im Detailbereich und als verknüpftes Element unter dem Container Domäne im Navigationsbereich angezeigt.
6. Sie können die Reihenfolge der verknüpften GPOs anpassen, um sicherzustellen, dass die GPOs mit höherer Priorität zuletzt verarbeitet werden. Wählen Sie ein GPO aus, und klicken Sie auf den Aufwärts- oder Abwärtspfeil, um es zu verschieben. Die GPOs werden vom Clientgerät von der höchsten Verknüpfungs Auftragsnummer bis zum niedrigsten verarbeitet.

Ändern der GPO-Filter für die Anwendung auf eine andere Zone oder Version von Windows

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

Sie müssen das kopierte GPO neu konfigurieren, damit es die richtige Sicherheitsgruppe und WMI-Filter für die neue Rolle enthält. Wenn Sie das Gruppenrichtlinienobjekt für die isolierte Domäne erstellen, verwenden Sie die Block Mitglieder einer Gruppe, um eine GPO -Prozedur anzuwenden, um zu verhindern, dass Mitglieder der Grenz-und Verschlüsselungs Zonen die GPOs für die Haupt isolierte Domäne falsch anwenden.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

In diesem Thema:

- Ändern des Sicherheitsgruppen Filters für ein GPO
- Blockieren der Anwendung eines Gruppenrichtlinienobjekts durch Mitglieder einer Gruppe
- Entfernen eines Blocks für Mitglieder einer Gruppe aus der Anwendung eines Gruppenrichtlinienobjekts

So ändern Sie den Sicherheitsgruppenfilter für ein GPO

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Suchen Sie im Navigationsbereich, und klicken Sie dann auf das Gruppenrichtlinienobjekt, das Sie ändern möchten.
3. Klicken Sie im Detailbereich unter **Sicherheitsfilterung**auf die aktuell zugewiesene Sicherheitsgruppe, und klicken Sie dann auf **Entfernen**.
4. Nun können Sie diesem GPO die entsprechende Sicherheitsgruppe hinzufügen. Klicken Sie unter **Sicherheitsfilterung**auf **Hinzufügen**.
5. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppe auswählen** den Namen der Gruppe ein, deren Mitglieder das Gruppenrichtlinienobjekt anwenden sollen, und klicken Sie dann auf **OK**. Wenn Sie den Namen nicht kennen, können Sie auf **erweitert** klicken, um die Liste der in der Domäne verfügbaren Gruppen zu durchsuchen.

So verhindern Sie, dass Mitglieder einer Gruppe ein Gruppenrichtlinienobjekt anwenden

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Suchen Sie im Navigationsbereich, und klicken Sie dann auf das Gruppenrichtlinienobjekt, das Sie ändern möchten.
3. Klicken Sie im Detailbereich auf die Registerkarte **Delegierung** .

4. Klicken Sie auf **Erweitert**.
5. Klicken Sie unter der Liste **Gruppen-oder Benutzernamen** auf **Hinzufügen**.
6. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppe auswählen** den Namen der Gruppe ein, deren Mitglieder daran gehindert werden sollen, das Gruppenrichtlinienobjekt anzuwenden, und klicken Sie dann auf **OK**. Wenn Sie den Namen nicht kennen, können Sie auf **erweitert** klicken, um die Liste der in der Domäne verfügbaren Gruppen zu durchsuchen.
7. Wählen Sie die Gruppe in der Liste **Gruppen-oder Benutzernamen** aus, und aktivieren Sie dann die Kontrollkästchen in der Spalte **verweigern** für die **Gruppenrichtlinie Lesen** und anwenden.
8. Klicken Sie auf **OK**, und klicken Sie dann im Dialogfeld **Windows-Sicherheit** auf **Ja**.
9. Die Gruppe wird in der Liste mit benutzerdefinierten Berechtigungen angezeigt.

So entfernen Sie einen Block für Mitglieder einer Gruppe aus der Anwendung eines Gruppenrichtlinienobjekts

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Suchen Sie im Navigationsbereich, und klicken Sie dann auf das Gruppenrichtlinienobjekt, das Sie ändern möchten.
3. Klicken Sie im Detailbereich auf die Registerkarte **Delegierung** .
4. Wählen Sie in der Liste **Gruppen und Benutzer** die Gruppe aus, die nicht mehr blockiert werden soll, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie im Meldungsfeld auf **OK**.

Öffnen der Gruppenrichtlinien-Verwaltungskonsole zu IP-Sicherheitsrichtlinien

07.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die Verfahren in diesem Leitfaden, die auf GPOs für frühere Versionen des Windows-Betriebssystems verweisen, weisen Sie an, mit dem Abschnitt IP-Sicherheitsrichtlinie in der Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console, GPMC) zu arbeiten.

So öffnen Sie ein GPO im Abschnitt IP-Sicherheitsrichtlinien

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:** *YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, erweitern Sie **Gruppenrichtlinienobjekte**, klicken Sie mit der rechten Maustaste auf das zu ändernde GPO, und klicken Sie dann auf **Bearbeiten**.
3. Erweitern Sie im Navigationsbereich des Gruppenrichtlinien-Verwaltungs-Editors **Computer Konfiguration**, erweitern Sie **Richtlinien**, erweitern Sie **Windows-Einstellungen**, erweitern Sie **Sicherheitseinstellungen**, und klicken Sie dann **auf aktive IP-Sicherheitsrichtlinien Directory (***IhrDomänenname***)**.

Öffnen der Gruppenrichtlinien-Verwaltungskonsole für die Windows Defender-Firewall

04.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

So öffnen Sie ein GPO für die Windows Defender-Firewall:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:** *YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, erweitern Sie **Gruppenrichtlinienobjekte**, klicken Sie mit der rechten Maustaste auf das zu ändernde GPO, und klicken Sie dann auf **Bearbeiten**.
3. Navigieren Sie im Navigationsbereich des Gruppenrichtlinienobjekt-Editors zu **Computerkonfigurations** > -**Administrative Vorlagen** > **Netzwerk** > **Netzwerkverbindungen** > **Windows Defender Firewall**.

Öffnen der Gruppenrichtlinien-Verwaltungskonsole zur Windows-Firewall mit erweiterter Sicherheit

07.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Die meisten Verfahren in diesem Leitfaden weisen Sie an, Gruppenrichtlinieneinstellungen für die Windows-Firewall mit erweiterter Sicherheit zu verwenden.

So öffnen Sie ein GPO für die Windows-Firewall mit erweiterter Sicherheit

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie im Navigationsbereich **Gesamtstruktur:** *YourForestName*, erweitern **Sie Domänen**, erweitern Sie *IhrDomänenname*, erweitern Sie **Gruppenrichtlinienobjekte**, klicken Sie mit der rechten Maustaste auf das zu ändernde GPO, und klicken Sie dann auf **Bearbeiten**.
3. Navigieren Sie im Navigationsbereich des Gruppenrichtlinien-Verwaltungs-Editors zu **** den Computerkonfigurations > **Richtlinien** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Windows-Firewall mit erweitertem Sicherheits** > **-Windows-Firewall mit erweiterter Sicherheit-LDAP://CN = {***GUID***}, CN =.**...

Öffnen der Windows Defender-Firewall mit erweiterter Sicherheit

31.12.2019 • 2 minutes to read

Betrifft:

- Windows 10
- Windows Server 2016

Dieses Verfahren zeigt, wie Sie die Windows Defender-Firewall mit erweiterter Sicherheitskonsole öffnen.

Administrative Anmeldeinformationen

Sie müssen ein Mitglied der Gruppe Administratoren sein, um dieses Verfahren ausführen zu können. Weitere Informationen finden Sie unter Weitere Überlegungen.

So öffnen Sie die Windows Defender-Firewall über die Benutzeroberfläche

Klicken Sie auf Start, geben Sie **Windows Defender Firewall**ein, und drücken Sie dann die EINGABETASTE.

So öffnen Sie die Windows Defender-Firewall über eine Eingabeaufforderung

1. Öffnen Sie ein Eingabeaufforderungsfenster.
2. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
wf.msc
```

Weitere Überlegungen

Obwohl Standardbenutzer das MMC-Snap-in Windows Defender Firewall starten können, muss der Benutzer ein Mitglied einer Gruppe mit den Berechtigungen zum Ändern dieser Einstellungen sein, beispielsweise Administratoren.

Einschränken des Serverzugriffs auf Mitglieder einer Gruppe

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie die IPsec-Verbindungssicherheitsregeln konfiguriert haben, die Clientgeräte zwingen, ihre Verbindungen mit dem isolierten Server zu authentifizieren, müssen Sie die Regeln konfigurieren, die den Zugriff auf die Geräte oder Benutzer beschränken, die über die Authentifizierungsprozess als Mitglieder der Access-Gruppe des isolierten Servers.

In diesem Thema:

- Erstellen einer Firewallregel für den Zugriff auf isolierte Server, auf denen Windows Server2008 oder höher ausgeführt wird

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So erstellen Sie eine Firewall-Regel, die Zugriff auf einen isolierten Server gewährt

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit. Sie müssen das Gruppenrichtlinienobjekt bearbeiten, das Einstellungen auf Server in der isolierten Serverzone anwendet.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Eingehende Regeln**, und klicken Sie dann auf **neue Regel**.
3. Klicken Sie **** auf der Seite Regeltyp auf **Benutzerdefiniert**, und klicken Sie dann auf **weiter**.
4. Wenn Sie den Zugriff auf ein einzelnes Netzwerkprogramm einschränken müssen, können Sie **diesen Programmpfad**auswählen und das Programm oder den Dienst angeben, dem Sie den Zugriff gewähren möchten. Klicken Sie andernfalls auf **Alle Programme**, und klicken Sie dann auf **weiter**.
5. Wenn Sie den Zugriff nur auf einige TCP-oder UDP-Portnummern beschränken müssen, geben Sie die Portnummern auf der Seite **Protokoll und Ports** ein. Setzen Sie andernfalls **** den Protokolltyp auf **any**, und klicken Sie dann auf **weiter**.
6. Wählen Sie **** auf der Seite Bereich **eine beliebige IP-Adresse** für lokale und Remoteadressen aus, und klicken Sie dann auf **weiter**.
7. Klicken Sie auf der Seite **Aktion** auf **Verbindung zulassen, wenn Sie sicher ist**. Wenn dies für Ihr Design erforderlich ist, können Sie auch auf **Anpassen** klicken und auswählen, dass **die Verbindungen verschlüsselt werden**müssen. Klicken Sie auf **Weiter**.
8. Aktivieren Sie auf der Seite **Benutzer und Computer** das Kontrollkästchen für den Typ der Konten (Computer oder Benutzer), die Sie zulassen möchten, klicken Sie auf **Hinzufügen**, und geben Sie dann das

Gruppenkonto ein, das die Geräte-und Benutzerkonten enthält, die für den Zugriff auf den Server zugelassen sind.

Aktivieren der Windows Defender-Firewall mit erweiterter Sicherheit und Konfigurieren des Standardverhaltens

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Zum Aktivieren der Windows Defender-Firewall mit erweiterter Sicherheit und zum Konfigurieren des Standardverhaltens verwenden Sie den Knoten Windows Defender-Firewall mit erweiterter Sicherheit in der Gruppenrichtlinien-Verwaltungskonsole.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So aktivieren Sie die Windows Defender-Firewall und konfigurieren das Standardverhalten

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole mit der Windows Defender-Firewall mit erweiterter Sicherheit.
2. Klicken Sie im Detailbereich im Abschnitt **Übersicht** auf Eigenschaften von **Windows Defender-Firewall**.
3. Führen Sie für jeden Netzwerkadresstyp (Domäne, privat, öffentlich) die folgenden Schritte aus.

   > **Hinweis:** die hier gezeigten Schritte geben die empfohlenen Werte für eine typische Bereitstellung an. Verwenden Sie die Einstellungen, die für Ihr Firewall-Design geeignet sind.

   a. Klicken Sie auf die Registerkarte, die dem Typ des Netzwerkspeicherorts entspricht.

   b. Ändern Sie den **Firewall-Status** auf **ein (empfohlen)**.

   c. Ändern Sie **eingehende Verbindungen** in **blockieren (Standard)**.

   d. Ändern Sie **ausgehende Verbindungen** in **zulassen (Standard)**.

Sicherstellen, dass der Netzwerkdatenverkehr authentifiziert wird

01.06.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

Nachdem Sie Ihre Domänenisolationsregel so konfiguriert haben, dass die Authentifizierung nicht erforderlich ist, müssen Sie sicherstellen, dass der von den Geräten im Netzwerk gesendete Netzwerkdatenverkehr wie erwartet durch die IPSec-Authentifizierung geschützt wird. Wenn Sie Ihre Regeln so umstellen, dass eine Authentifizierung erforderlich ist, bevor alle Geräte die richtigen GPOs empfangen und angewendet haben, oder wenn in ihren Regeln Fehler auftreten, kann die Kommunikation im Netzwerk fehlschlagen. Wenn Sie zuerst die Regeln zum Anfordern der Authentifizierung festlegen, können Netzwerkverbindungen, bei denen die Authentifizierung fehlschlägt, in Klartext fortgesetzt werden, während Sie diagnostizieren und beheben.

In diesen Verfahren bestätigen Sie, dass die von Ihnen bereitgestellten Regeln ordnungsgemäß funktionieren. Die nächsten Schritte hängen von der Zone ab, an der Sie arbeiten:

- **Hauptdomänen-Isolierungs Zone.** Bevor Sie Ihre Hauptdomänen Isolierungs-IPSec-Regel aus dem Anforderungsmodus in den require-Modus konvertieren, müssen Sie sicherstellen, dass der Netzwerkdatenverkehr entsprechend Ihrem Entwurf geschützt ist. Indem Sie Ihre Regeln so konfigurieren, dass zu Beginn des Vorgangs eine Authentifizierung angefordert wird und keine Authentifizierung erforderlich ist, können Geräte im Netzwerk weiterhin kommunizieren, auch wenn die Hauptmodus-Authentifizierung oder die Integritäts-und Verschlüsselungsregeln für den Schnellmodus nicht ordnungsgemäß funktionieren. Wenn Ihre Verschlüsselungszone beispielsweise Regeln enthält, die einen bestimmten Verschlüsselungsalgorithmus erfordern, dieser Algorithmus aber nicht in einer Kombination aus Sicherheitsmethoden auf den Clients enthalten ist, können diese Clients keine Schnellmodus-Sicherheitszuordnung erfolgreich aushandeln. , und der Server weigert sich, den Netzwerkdatenverkehr vom Client zu akzeptieren. Wenn Sie zunächst nur den Anforderungsmodus verwenden, können Sie Ihre Regeln bereitstellen und dann den Netzwerkdatenverkehr überprüfen, um festzustellen, ob Sie wie erwartet funktionieren, ohne den Verlust von Kommunikation zu riskieren.
- **Grenz Zone.** Die Bestätigung der korrekten Funktion von IPSec ist der letzte Schritt, wenn Sie an dem Gruppenrichtlinienobjekt für Grenzzonen arbeiten. Sie konvertieren das Gruppenrichtlinienobjekt nicht in den require-Modus.
- **Verschlüsselungszone.** Ähnlich wie bei der Haupt Isolierungs Zone müssen Sie, nachdem Sie bestätigt haben, dass der Netzwerkdatenverkehr zu Zone-Mitgliedern ordnungsgemäß authentifiziert und verschlüsselt ist, ihre Zonenregeln aus dem Anforderungsmodus in den require-Modus konvertieren.

> **Hinweis:** zusätzlich zu den in diesem Verfahren gezeigten Schritten können Sie auch Tools zum Aufzeichnen von https://go.microsoft.com/fwlink/?linkid=94770Netzwerkdatenverkehr verwenden, wie beispielsweise den Microsoft-Netzwerk Monitor, der heruntergeladen werden kann. Mit dem Netzwerk Monitor und ähnlichen Tools können Sie die Netzwerkpakete, die vom Netzwerkadapter auf Ihrem Gerät empfangen werden, erfassen, analysieren und anzeigen. Die aktuellen Versionen dieser Tools umfassen die vollständige Unterstützung für IPSec. Sie können verschlüsselte Netzwerkpakete identifizieren, aber nicht entschlüsseln.

Administrative Anmeldeinformationen

Um diese Schritte ausführen zu können, müssen Sie ein Mitglied der Gruppe der Domänenadministratoren sein oder anderweitig über die Berechtigung zum Ändern der GPOs verfügen.

So überprüfen Sie, ob Netzwerkverbindungen mithilfe der Windows Defender-Firewall mit erweiterter Sicherheitskonsole authentifiziert werden

1. Öffnen Sie die Windows Defender-Firewall mit erweiterter Sicherheitskonsole.
2. Erweitern Sie im Navigationsbereich **Überwachung**, und klicken Sie dann auf **Verbindungssicherheitsregeln**.

   Im Detailbereich werden die aktuell auf dem Gerät gültigen Regeln angezeigt.
3. **So zeigen Sie die Spalte "Regelquelle" an**

   a. Klicken Sie im Bereich **Aktionen** auf **Ansicht**, und klicken Sie dann auf **Spalten hinzufügen/entfernen**.

   b. Wählen Sie in der Liste **Verfügbare Spalten** die Option **Regelquelle**aus, und klicken Sie dann auf **Hinzufügen**.

   c. Verwenden Sie die Schaltflächen nach **oben** und nach **unten** , um die Reihenfolge neu anzuordnen. Klicken Sie abschließend auf **OK** .

   Es kann einige Minuten dauern, bis die Liste mit der neu hinzugefügten Spalte aktualisiert wird.
4. Überprüfen Sie die Liste der Regeln von GPOs, die auf dieses Gerät angewendet werden sollen.

   > **Hinweis:** wenn die Regeln nicht in der Liste angezeigt werden, beheben Sie die Problembehandlung für die Gruppenrichtlinienobjekt-Sicherheitsgruppe und die WMI-Filter, die auf das Gruppenrichtlinienobjekt angewendet werden. Stellen Sie sicher, dass das lokale Gerät Mitglied der entsprechenden Gruppen ist und die Anforderungen der WMI-Filter erfüllt.

5. Erweitern Sie im Navigationsbereich **Sicherheitszuordnungen**, und klicken Sie dann auf **Hauptmodus**.

   Die aktuelle Liste der Hauptmodus-Zuordnungen, die mit anderen Geräten ausgehandelt wurden, wird in der Spalte Details angezeigt.
6. Überprüfen Sie die Liste der Hauptmodus-Sicherheitszuordnungen für Sitzungen zwischen dem lokalen Gerät und dem Remotegerät. Stellen Sie sicher, dass die Spalten **Erste Authentifizierungsmethode** und **zweite Authentifizierungsmethode** die erwarteten Werte enthalten. Wenn Ihre Regeln nur eine erste Authentifizierungsmethode angeben, wird in der Spalte **2. Authentifizierungsmethode keine Authentifizierung**angezeigt. Wenn Sie auf die Zeile doppelklicken, wird das Dialogfeld **Eigenschaften** mit zusätzlichen Details zur Sicherheitszuordnung angezeigt.
7. Klicken Sie im Navigationsbereich auf **Schnellmodus**.
8. Überprüfen Sie die Liste der Schnellmodus-Sicherheitszuordnungen für Sitzungen zwischen dem lokalen Gerät und dem Remotegerät. Stellen Sie sicher, dass die Spalten **AH-Integrität**, **ESP-Integrität**und ESP-**Vertraulichkeit** erwartete Werte enthalten.